

**PX 42**

Message

---

**From:** Antoinette O'Gorman [REDACTED]@ripple.com]  
**on behalf of** Antoinette O'Gorman <[REDACTED]@ripple.com> [REDACTED]@ripple.com]  
**Sent:** 11/21/2016 1:56:40 PM  
**To:** [REDACTED] [REDACTED]@ripple.com]  
**Subject:** For Audit-related question - Compliance-related policies  
**Attachments:** 2016 Code of Conduct.pdf; 2016 Code Acknowledgment.pdf; Final Dec 2015 XRP II AML Program.pdf; Compliance Program April 2016 Final.pdf; Vendor Management Policy Rev April 2016.pdf

As I mentioned, their question on audits performed to ensure compliance with legal, regulatory requirements may also include reference to any independent financial audits conducted on Ripple and/or its subsidiaries. The requirement for annual independent BSA audits is referenced in XRP II's AML Program (see page 18) and is a requirement of any financial services business.

Our Code of Conduct Policy references Ripple's requirement of all existing employees to notify Ripple senior management of any violation of policy and/or law (see section 7).

Antoinette O'Gorman  
Chief Compliance Officer | Ripple  
[REDACTED]@ripple.com | ripple.com



# Acknowledgement Form

I acknowledge receipt of Ripple's Code of Conduct (the "Code"). I further acknowledge that I have read, understood and agree to abide by the terms of the Code.

---

Signature

---

Name

---

Date



# Ripple Code of Conduct

December 2015



## Overview

We have four primary values that represent what Ripple believes as a team and form the basis for everything we do:

**Openness:** Ripple is an open-source protocol. We value transparency with each other and with the world.

**Constructiveness:** We are builders, not disruptors. The Ripple protocol provides the technology infrastructure onto which new payment systems can emerge and established payment systems, regulations, and institutions can migrate.

**Inclusiveness:** Ripple does not discriminate in hiring and engineering practices. We build for the world, not just for ourselves.

**Humility:** Ripple recognizes that developers and enterprises are the true innovators building and expanding the value web. Employees of Ripple are not focused on who is right; rather, what is right.



## Introduction

The reputation and good name of Ripple depend entirely upon the honesty and integrity of each employee and all those closely associated with the company.

This Code of Conduct applies in its entirety to all Ripple employees. Certain provisions of the Code of Conduct appropriately extend beyond employees to cover the Board of Directors, contractors, founders, investors, and advisors ("Insiders").

It is impossible to cite examples of every type of activity that might give rise to a question of unethical conduct. Therefore, it is important that each employee and every Insider to the company exercise good judgment in the performance of his or her duties and responsibilities. When situations occur where the proper course of action is unclear, employees must request advice and counsel from their managers or from the Head of HR / People Operations at Ripple, who can be contacted via email at [hr@ripple.com](mailto:hr@ripple.com). Contractors in need of advice regarding ethical questions should consult their engagement officer at Ripple, and other Insiders should consult with the Board.

## 1. Treating Others with Dignity and Respect

We are committed to fostering an inclusive workplace where talented people want to stay and develop their careers. Supporting a diverse, engaged workforce allows us to be successful in building trust, empowering teams, serving our clients and outperforming our peers. We give equal employment opportunity to all individuals in compliance with legal requirements and because it's the right thing to do.

Respecting others, appreciating diverse points of view and making decisions based on merit are predicated on our core values. Our policy ensures equal employment opportunity without discrimination or harassment on the basis of race, color, religion, age, gender, gender identity, sexual orientation, national origin, citizenship, disability, marital and civil partnership and union status, pregnancy (including unlawful discrimination on the basis of a legally protected pregnancy or maternity leave), veteran status or any other characteristic protected by law.

We expect that all relationships in the workplace will be free of bias, harassment and violence.

Ripple strictly prohibits and will not tolerate any form of sexual harassment or job discrimination. Such conduct is unacceptable in the workplace as well as in any work-related setting outside of the workplace.

## Ethical Decision-Making

Each of us has a responsibility to uphold the Code; in fact, compliance with the Code is a term and condition of employment with the Company. This means you must do the right thing when it comes to your own conduct, and you must speak up about conduct of others that might violate our Code of Conduct or Company policies. It also means you must cooperate as directed by the Company with any investigation, inquiry, examination or litigation related to the Company's business. Upon joining the Company, new hires are required to provide



affirmation that they have read and understand the Code, will comply with it, and will report any suspected violations, as required. New hires are required to complete Code of Conduct training shortly after beginning work at Ripple. Compliance with these requirements is a condition of employment.

## Manager Responsibilities

Managers have an even greater level of responsibility. If you are a manager, your employees look to you to lead with integrity. Make sure you know the Code and can either help employees with questions or direct them to someone who can. If an ethical issue or a suspected violation is brought to your attention, don't investigate it yourself. You can report it using Ripple's anonymous reporting hotline (via phone [REDACTED] or online at [www.ripple.ethicspoint.com](http://www.ripple.ethicspoint.com)) and ask the employee who came forth to do the same. The matter will be investigated by an appropriate party, such as Human Resources, Compliance, or Legal. Managers are responsible for supervising the activities and conduct of employees in their reporting line and should always make sure that the reporting employee is protected from any form of retaliation. Consult with People Operations when you identify a concern or misconduct or on how to prevent its recurrence. Managers who fail to take action and report misconduct may be held responsible for their failure to report or failure to take steps to address or remediate an identified issue.

## Compliance with the Law

Being aware of — and complying with — the laws and regulations under which we operate is not just a critical part of our business, but fundamental to who we are. It is important to comply with not just the letter, but also the spirit and intent, of the law. Violating the law — or engaging in unfair, deceptive and abusive acts or practices — may weaken customer confidence and put our reputation at risk, and can result in regulator criticism, legal action, fines and penalties, and other negative repercussions for our Company. If complying with any provision of our Code would cause you to violate local law, you should follow the local law. As an employee, you are expected to know and comply with the laws and regulations that apply to you and, if you ever have questions, to contact your Compliance Officer or People Operations for help.

## 2. Insider Purchase, Sale and Holdings of XRP

### XRP and the Ripple Protocol

XRP is a math-based currency that is native to the Ripple protocol. The inventors of the Ripple protocol created 100 billion XRP at its inception, and gifted 80 billion of the 100 billion XRP to Ripple. No more can ever be created according to the protocol's rules.

Ripple reserves approximately 25 billion XRP to fund its operations, and distributes the balance. Our goal in distributing XRP is to incentivize actions that build trust, utility and liquidity in Ripple.



## Acting Ethically and Transparently

It is imperative that all Ripple employees, contractors, founders, Board members, investors, and advisors act ethically and transparently with respect to purchases, sales, and holdings of XRP, in alignment with the goal of building and maintaining public trust in Ripple.

### **Purchase, Sale and Disclosure of Holding XRP**

The following requirements apply to all Ripple Insiders:

**XRP Giveaways** - Insiders may not participate in XRP "giveaways" hosted or promoted by the Company.

**Purchase and Sale of XRP** - Insiders should avoid activity that could impair the integrity or reputation of Ripple or disadvantage other users of the protocol. For this reason:

- Insiders may not buy, sell, recommend or trade XRP, either personally or on behalf of someone else, under circumstances that could appear unfair to the wider Ripple community and non-Insiders generally. This includes situations in which Insiders have access to information about Ripple or the Ripple protocol that has not been publicly announced, and which might reasonably affect the decision to buy or sell XRP.
- The Company may from time to time designate certain time periods as "restricted" periods if in the judgment of executive management, a coming announcement or other event may significantly affect the trading price of XRP. During such restricted periods, Insiders may not buy, sell, trade or recommend XRP. At other times, Insiders are responsible for exercising their judgment as to whether trading XRP is appropriate.
- Insiders may not buy, sell, recommend, or trade XRP valued in excess of \$100,000 in any one month, either personally or on behalf of someone else, without prior written approval from Ripple's CFO, the Chief Compliance Officer, and a direct supervisor. If the XRP transaction does not occur within one month of authorization, re-approval must be sought.

Following are examples of situations in which it would be inappropriate for Insiders to buy, sell, trade, or recommend XRP:

- Prior to public announcements of new bank partnerships
- Prior to public announcements relating to adverse regulatory actions
- Prior to public announcements regarding other significant partnerships (e.g., financial coalitions)
- Prior to public announcements relating to CEO or founders' XRP movement

Following are examples of situations in which it would be appropriate for Insiders to buy, sell, trade, or recommend XRP:

- Purchasing XRP pursuant to a documented automatic investment program, or a standing order locked in at a specific price
- Small transactions in regular course of business (under \$3,000 or the equivalent in XRP)
- Purchasing (less than \$100,000 worth of XRP per month) due to general confidence in Ripple team members, and confidence in the Company itself

Failure to comply with these restrictions may be grounds for disciplinary action, including termination of association with Ripple. Depending on the severity of the breach of fiduciary responsibility, further legal and financial penalties may apply.



### 3. Compliance with Anti-Money Laundering Laws

The following provision applies to all Ripple Insiders:

Ripple is firmly committed to the prevention of money laundering and terrorist financing activities, and to compliance with applicable anti-money laundering laws, including the Bank Secrecy Act and the USA PATRIOT Act. Ripple's Anti-Money Laundering Policy is also designed to achieve compliance with the U.S. Office of Foreign Assets Control ("OFAC" or, more broadly, "sanctions") regulations. Money laundering is the process by which individuals attempt to conceal the true origin and ownership of the proceeds of illegal activities. If undertaken successfully, control may be maintained over the proceeds, and ultimately, a cover provided for the source of illegal activities. Violating these laws is strictly prohibited. As a member of the financial services community, you have a special obligation to support law enforcement throughout the world to combat various types of financial crime, such as attempts to launder money for criminal activity and finance terrorist operations. You're expected to comply fully with all anti-money laundering laws and only conduct business with reputable entities involved in legitimate business activities that use funds derived from lawful purposes.

Failure to comply with anti-money laundering laws puts the company and you at serious risk and may be grounds for disciplinary action, including termination of association with Ripple. Depending on the severity of the breach of fiduciary responsibility, the company may report such activities to governmental agencies, and further legal and financial penalties may apply.

#### Anti-Bribery and Corruption:

Ripple's reputation for integrity is central to the success of our business. We will never compromise our reputation by engaging in, or appearing to engage in, bribery or any form of corruption. Employees or Insiders may not give, offer or promise (directly or through others such as family members) anything of value to government officials, clients, suppliers or other business partners, if it is intended or could reasonably appear as intended to obtain some improper business advantage.

Ripple employees or insiders may not solicit or accept anything of value (either directly or through others such as family members) if it is intended or could reasonably appear as intended to improperly influence your decisions on behalf of Ripple. Ripple's Anti-Bribery and Corruption Policy also prohibits facilitation or "grease" payments which include anything of value given to a foreign government official to cause that government official to perform a routine duty or function, or to expedite such performance. Refer to Ripple's Anti-Bribery and Corruption Policy for additional details.

Ripple expects all employees to act ethically and does not tolerate bribery. If something seems improper or may involve bribery, contact your Compliance Officer or submit a report:

- using Ripple's Internal Unusual Activity Reporting ("UAR") process;
- via Ripple's global reporting hotline – telephone [REDACTED] (anonymous reporting); or,
- online at [www.ripple.ethicspoint.com](http://www.ripple.ethicspoint.com) (anonymous reporting)



## 4. Company Property and Information

The following provision applies to all Ripple Insiders:

**Company Property:** An employee has a duty to protect and conserve Company property and ensure its use for proper purposes.

**Company Information:** Ripple created and supports the Ripple protocol, an open-source, distributed payments protocol. This work of Ripple includes producing additional open source software products for use by developers and users of the network. While we do strive to be as open as possible, we do maintain certain confidential information.

Knowing what information should be kept confidential and what can be disclosed is a skill that every employee and all other Insiders should master. When in doubt about the confidentiality of particular information, employees and contractors should verify with an officer of Ripple that the information can be shared before doing so; other Insiders should consult with the CEO or a member of the Board.

Employees and other Insiders must strictly preserve the confidentiality of non-public information to which they have access that is designated as confidential, private or proprietary. It can be disclosed only as required for Company purposes and only as authorized.

**Use of Non-Public Information for Private Gain:** Employees and other Insiders may not use non-public information for any purpose other than Ripple business. An employee or other Insider may not allow the improper use of such non-public information to further his or her own private interest or that of another person, whether through advice, recommendation, or a knowing, unauthorized disclosure.

**Dealing with Confidential Information:** Trust is essential to our business success. Customers, companies and business partners with which we do business trust us to be good stewards of their confidential information, whether that information relates to financial, personal or business matters. Confidential information can be written, oral, telephonic or electronic and includes a wide variety of data, from technology applications, business strategies and customer lists to personnel information.

How do you know what information is confidential information? The best practice is to assume that all personal information and all information you have about the Company and its business (including past, present and prospective customers, business partners, directors and employees) is confidential, unless the contrary is clear. Disclose confidential information only on a need-to-know basis. You have a duty to protect confidential information and to take precautions before sharing it with anyone, inside or outside the workplace.

- Don't share confidential information with friends or family, and don't discuss it in places where others could overhear.
- Don't access or use confidential information, and don't disclose it to fellow employees who are not involved in providing services to the owner of the information, unless you are authorized and legally permitted to do so.

Finally, don't send confidential information, including internal communications such as intranet



postings, outside the Company (including to your own personal email address), unless permitted to do so under applicable law and Company policy or procedures.

We are also obliged to safeguard confidential information of prior employers. Your responsibility to protect confidential information also applies to work you may have done before coming to Ripple. Sharing confidential information from a former employer is unethical and can also expose you and Ripple to legal liabilities. Do not disclose any confidential information of a prior employer unless it's already been made public through no action of your own.

Each of us has a special responsibility to protect the confidentiality of information related to our customers. This responsibility may be imposed by law, may arise out of agreements with our customers or may be based on policies or practices adopted by the Company. Certain jurisdictions have regulations relating specifically to the privacy of individuals and business customers.

## 5. Conflicts of Interest

The term "conflict of interest" describes any circumstances that could cast doubt on an Insider's ability to act with objectivity with regard to Ripple's interest. The following provision applies to all Ripple Insiders, who are expected to avoid actions or involvements that could compromise their ability to act on behalf of Ripple.

Determining whether a conflict of interest exists is not always easy to do. Employees with a conflict of interest question should seek advice and guidance from their manager. Before engaging in any activity, transaction or relationship that might give rise to a conflict of interest, employees must seek review from their managers or People Operations.

Activities that could raise a question of conflict of interest include, but are not limited to, the following:

- Conduct business on behalf of Ripple with a member of the Insider's family or a business organization in which the Insider or a member of his or her family has a significant association, which could give rise to a conflict of interest, without first obtaining written approval. Employees and contractors should obtain such approval from an officer of Ripple; other Insiders should obtain approval from the Board.
- Serve as a director, board member or in an advisory or consultative, technical or managerial capacity for any non-affiliated business organization, government agency or industry group that interacts or does business with Ripple, is a competitor of Ripple, or is a client of Ripple without disclosing that affiliation. Employees and contractors should disclose such affiliations to People Operations; other Insiders should disclose such affiliations to the Board.
- Accept any position outside Ripple, which interferes with the proper performance of his or her duties.
- Take advantage of any business opportunity, which might be of interest to Ripple.



**Disclosure of Investments:** Ripple employees will disclose to People Operations all investments in (1) third party companies that make material use of the Ripple protocol, or that interoperate with others that do so, and (2) competitors of Ripple. Employees and contractors should disclose such investments to the People Operations area of Ripple; other Insiders should disclose such investments to the Board. Ripple may at its discretion share disclosures of investments in third party companies with various audiences, including the media, other investors and advisors, or the management of incubator programs with which Ripple is associated.

**Gifts, Gratuities and Business Courtesies:** The exchange of gifts and offers of entertainment are common business practices, but too often can be misinterpreted or suggest the appearance of something improper, even when there is no improper intent. While business gifts and entertainment can be important to building goodwill, they can also affect the relationship if your ability to exercise sound business judgment becomes blurred. The inappropriate giving or receiving of gifts and entertainment can erode the distinction between a business and a personal relationship. Ripple employees should avoid any actions that create a perception that favorable treatment of outside entities by the company was sought, received or given in exchange for personal business courtesies. Business courtesies include gifts, gratuities, meals, refreshments, entertainment or other benefits from persons or companies with whom Ripple does or may do business. Ripple will neither give nor accept business courtesies that constitute, or could reasonably be perceived as constituting, unfair business inducements that would violate law, regulation or the company's reputation.

A gift is anything of value and can take many forms, including meals or refreshments; goods or services; tickets to entertainment or sporting events; the use of a residence, vacation home or other accommodations; a raffle prize; travel expenses; a product or service discount; or charitable or political contributions made on your behalf. In general, anytime a recipient is not required to pay the retail or customary cost for something, it is considered a "gift." Also keep in mind that gifts given by others to members of your family or to those with whom you have a close personal relationship or to charities designated by you are considered to be gifts to you.

**Giving Gifts:** Offering gifts may be acceptable unless intended to improperly influence a business decision. Make sure that any gifts you offer are reasonable and customary and conform to our Code and Company policies. In general, you should never give a gift that:

- Would violate local laws, industry-specific regulations or the policies of the recipient
- Is intended or could reasonably appear as intended to obtain an improper business advantage
- Could appear to be offered with the intent of influencing someone to do something improper
- Would be considered lavish or inappropriate under the circumstances

Gift giving to government officials is governed by very strict laws and regulations, violations of which can have severe consequences for both you and the Company.

**Accepting Gifts** - From time to time, you may be offered gifts from a customer, company or person doing — or seeking to do — business with Ripple. In general, you should not accept gifts of any kind, but there are certain situations where it is permissible. Start by asking yourself:



1. Did I solicit the gift?
2. Have I received frequent gifts or offers from this same source?
3. Would acceptance of it violate any Company policies?
4. Is this gift being given in appreciation for good service or as thanks for the Company's business?
5. Is this customer, supplier or company trying to influence or reward me in connection with a business decision or transaction?

If the answer to all five questions is "no," you may accept a gift with a retail value of USD\$100 or less given on an occasion when gifts are customary.

If you receive a gift that is not permitted by policy, you have a responsibility to politely refuse or return it.

## 6. Post-Employment Activities

The following provision applies to all Ripple employees:

**Non-public Information:** An employee's duty to maintain the confidentiality of non-public information continues after his or her employment ends. This information pertains not only to our Company but to those individuals and companies that do business with us; this does not prevent you from reporting to the government or regulators conduct that you believe to be in violation of law.

All Company assets in your possession must be returned to the Company. An employee must leave all Company laptops, documents, files, computers, reports and records containing non-public information, and all copies of such information, with the Company when his or her employment ends.

**Solicitation of Employees:** Upon leaving Ripple, former employees shall not seek to solicit employees of Ripple nor take any action to persuade employees to terminate their employment with Ripple for a period of twelve months.

## 7. Reporting and Required Absences

The following provision applies to all Ripple employees:

**Reporting Violations of Law and Policy:** Employees are encouraged to report violations of the law or Company policy. We encourage employees to ask questions and have open conversations with their managers on business and conduct concerns. We rely on our



employees to speak up when something is unclear. You are required to promptly report any known or suspected violations of the Code, any internal Company policy or any law or regulation related to our business. Reporting is required whether the violation involves you or someone else subject to the Code. You should report any known or suspected illegal conduct, or conduct that violates the underlying principles of the Code, by any of our customers, consultants, contract or temporary workers, business partners or agents. Just as you will be held responsible for your own actions, you can also be held responsible for not reporting the actions of others if you knew (or should have known) that they were in violation of any applicable policy, law or regulation.

In addition, your reporting obligations to the Company do not prevent you from reporting to the government or regulators conduct that you believe to be in violation of law. Violations should be reported to either:

- Chief Executive Officer, Chris Larsen;
- Chief Compliance Officer, Antoinette O’Gorman;
- via Ripple’s Unusual Activity Reporting (“UAR”) process, where appropriate; or,
- anonymously via Ripple’s Global reporting hotline: via phone [REDACTED] or online at [www.ripple.ethicspoint.com](http://www.ripple.ethicspoint.com) (Navex Global is a firm that supports company Compliance programs by offering a wide variety of services, including hotline reporting).

All reports will be treated confidentially to the maximum extent consistent with the fair and rigorous enforcement of these standards. When Ripple investigates any report of a violation of the Code of Conduct every employee must fully cooperate with the investigation, consistent with the employee’s rights under the law. Ripple will not permit retaliation against any employee for reporting potential violations.

**Report Criminal, Legal or Regulatory Proceedings that Involve You Personally:**

You must immediately report to People Operations the following incidents that involve you personally, whether they relate to the business of the Company or not:

- Any inquiry or action by a financial services regulator, law enforcement agency or similar authority, including any denial or suspension of a license or request seeking to take testimony or interview you regarding conduct at the Company or any other financial services institution;
- Any legal claims against you asserting fraud, dishonesty, or unfair or unethical conduct related to financial services.

If you have questions on whether you need to report a criminal, legal or regulatory proceeding, contact People Operations.



## 8. Employee Privacy

Ripple does not share employees' or other Insiders' personal information with companies, organizations or individuals outside the company without advance permission unless one of the following circumstances applies:

- We believe that is reasonably necessary to comply with a law, regulation or legal request
- To protect the safety of any person
- To address fraud, security or technical issues
- To protect Ripple's rights or property

However, nothing in this Policy is intended to limit any legal defenses or objections that you may have to a third party's, including a government's, request to disclose your information.

Ripple's policy is, when possible, to notify employees of requests for their account information, which includes a copy of the request, prior to disclosure, unless we are prohibited from doing so (e.g., an order under 18 U.S.C. § 2705(b)). Exceptions to prior notice may include exigent or counterproductive circumstances (e.g., emergencies; account compromises).



---

Ripple Labs, Inc. Compliance Policy

---

**RIPPLE LABS, INC.**  
**GENERAL COMPLIANCE POLICY**

**Related Documents**

<b>Title</b>	<b>Contact</b>
Code of Conduct	Chief Compliance Officer
Vendor Risk Management Policy	Chief Compliance Officer
Recordkeeping Policy	Chief Compliance Officer
New Product Risk Evaluation Process ("PREP")	VP, Product
Anti-Corruption/Anti-Bribery Program	Chief Compliance Officer
BSA/AML/OFAC Policy and Program	Chief Compliance Officer
Compliance Testing Guidelines	Chief Compliance Officer

**Owner:** Chief Compliance Officer | Antoinette O’Gorman

**Issue Date:** May 2016

**Contact:** Senior Compliance Manager, I [REDACTED]  
| [REDACTED]@ripple.com



*Ripple Labs Inc. All Rights Reserved.*

Table of Contents

1. INTRODUCTION ..... 4

2. POLICY OBJECTIVES ..... 4

3. SCOPE ..... 5

4. GOVERNANCE, ROLES AND RESPONSIBILITIES ..... 6

5. KEY TERMS ..... 8

6. THE POLICY ..... 9

7. RECORD RETENTION ..... 14

8. POLICY ADMINISTRATION ..... 15



Ripple Labs Inc. All Rights Reserved.



*Ripple Labs Inc. All Rights Reserved.*

## 1. INTRODUCTION

This Compliance Policy (the “Policy”) establishes a program to enable Ripple Labs, Inc. and its affiliates (collectively “Ripple”) achieve and maintain full compliance with financial services-related laws, regulations, and policies governing conduct of the businesses in which it engages (“Compliance Obligations”).

Consistent with this objective, Ripple has established a compliance risk management program that reflects industry best practice and regulatory guidance. This Policy outlines Ripple’s objectives, describes the scope of the program, and provides an overview of the major functions and responsibilities within the compliance framework.

In addition, Ripple has established an independent program to fully and continuously manage compliance with Bank Secrecy Act/Anti-Money Laundering (“BSA/AML”) and Office of Foreign Assets Control (“OFAC” or, more broadly, “sanctions”) legislation and regulations. Those program requirements are described separately in Ripple’s money services business subsidiaries’ “BSA/AML/OFAC Program”.

## 2. POLICY OBJECTIVES

The Compliance Policy seeks to ensure that all Ripple Compliance Obligations are identified in a timely manner and that processes by which compliance with those obligations will be achieved are effectively incorporated into ongoing business activities. Specifically, the objectives of this Policy include:

- Promoting and achieving a strong culture of compliance throughout Ripple;
- Ensuring that Ripple unfailingly meets its compliance obligations;
- Executing a Compliance Program that is consistently followed throughout Ripple;



*Ripple Labs Inc. All Rights Reserved.*

- Detecting, addressing, and reporting any significant compliance weaknesses or failures promptly and appropriately;
- Providing guidance to Ripple management and staff in the form of policies, procedures and training to impart a working understanding of the laws, regulations and policies associated with their responsibilities; and
- Maintaining a compliance function that is both independent and effective.

### 3. SCOPE

The Compliance Policy applies to any Compliance Obligation typically executed by internal Ripple departments relating to:

- Ethics and conduct;
- Privacy;
- Transaction-related issues;
- Other financial services-related laws and regulations; and
- Anti-money laundering requirements (addressed separately in Ripple's BSA/AML/OFAC Program).

Control areas other than Compliance have principal responsibility for risk management efforts regarding certain laws, regulations and policies outside the scope of Compliance Obligations. Compliance risk management activities with respect to the following requirements are outside the scope of this Policy:

- Credit, liquidity, operational and market risk-related regulatory requirements (Risk Management);
- Board governance, shareholder, and corporate-structure related regulatory requirements (Legal);
- Accounting and financial reporting and disclosure-related regulatory requirements (Controller);
- Employment-related requirements (Human Resources);



*Ripple Labs Inc. All Rights Reserved.*

- Tax-related requirements (Controller and Legal);
- Health and safety requirements (Human Resources);
- Information security requirements (Information Security Officer);
- Physical security requirements (Facilities); and
- Business continuity planning (Operations).

#### 4. GOVERNANCE, ROLES AND RESPONSIBILITIES

PARTY	ROLE/RESPONSIBILITY
<b>Policy Owner</b>	<p>The Chief Compliance Officer is responsible for:</p> <ul style="list-style-type: none"> <li>• Implementing and maintaining this Policy and related policies and procedures;</li> <li>• Proposing a risk-based, annual Compliance Plan that prioritizes compliance obligations, testing plans, and training-based risk assessment;</li> <li>• Implementing an approach for identification and assessment of compliance obligations, and coordinating risk assessments across internal departments;</li> <li>• Performing compliance testing of and monitoring adherence to the Compliance Policy throughout Ripple;</li> <li>• Reviewing any new products and services, assessing their compliance risk(s), and recommending mitigation strategies;</li> <li>• Identifying and assessing emerging compliance issues;</li> <li>• Promptly alerting senior management, the Compliance Oversight Committee, and the Board to material issues of non-compliance, and instituting and monitoring corrective action;</li> <li>• Chairing Compliance Oversight Committee meetings;</li> </ul>



Ripple Labs Inc. All Rights Reserved.

	<ul style="list-style-type: none"> <li>• Providing periodic reporting to senior management, the Compliance Oversight Committee, and the Board on the state of compliance and any significant emerging issues;</li> <li>• Coordinating audit and examination preparation and ensuring timely and comprehensive responses to audits/examinations involving compliance.</li> </ul>
<b>Governing Committees</b>	<p>The Compliance Oversight Committee is responsible for:</p> <ul style="list-style-type: none"> <li>• Promoting a strong culture of compliance;</li> <li>• Reviewing and approving the annual Compliance Plan;</li> <li>• Reviewing and approving this Policy and other key compliance policies;</li> <li>• Reviewing periodic compliance reports, including the state of compliance and testing and monitoring reports;</li> <li>• Reviewing and approving company-wide compliance initiatives;</li> <li>• Reviewing the scope and results of regulatory examinations or correspondence relating to Ripple's compliance program;</li> <li>• Monitoring corrective action and resolving escalated issues; and</li> <li>• Providing support to the Chief Compliance Officer on matters relating to audits and examinations.</li> </ul> <p>The Board of Directors is responsible for:</p> <ul style="list-style-type: none"> <li>• Ensuring that Ripple has adequate compliance resources and that the Chief Compliance Officer is independent of management;</li> <li>• Reviewing any escalated compliance reports and issues, including plans for corrective action; and</li> <li>• Reviewing the scope and results of regulatory examinations or correspondence relating to Ripple's compliance activities.</li> </ul>



Ripple Labs Inc. All Rights Reserved.

<b>Internal Departments</b>	<p>Internal departments affected by this Policy have principal accountability for ensuring implementation of appropriate compliance risk management in their areas. Internal department leaders should:</p> <ul style="list-style-type: none"> <li>• Promote a strong culture of compliance within their departments;</li> <li>• Implement this Policy within their areas of responsibility, including any necessary control activities;</li> <li>• Identify compliance weaknesses through monitoring activities, and promptly alert and work with Compliance to take corrective action;</li> <li>• Ensure that their staff receive appropriate compliance training; and</li> <li>• Allow Compliance personnel unrestricted access to any business records, systems, or locations necessary to fulfill the duties described in this Policy.</li> </ul>
<b>Legal</b>	<p>The Legal department is responsible for interpretation of financial services-related laws and regulations and for providing strategic advice to the Compliance team, as needed.</p>
<b>Human Resources</b>	<p>The Human Resources department assists with the development and administration of Ripple's Code of Conduct and with execution of the annual Compliance training program.</p>

## 5. KEY TERMS

Ripple assesses its compliance risk by rating the levels of inherent risk, control effectiveness, and residual risk. Each is defined as follows:

**Inherent risk** – the level of risk of potential non-compliance with a law, regulation, or rule and the possible impact – regulatory, reputational, legal, operational, and financial – resulting from non-compliance. Inherent risk does not take into account



*Ripple Labs Inc. All Rights Reserved.*

the effectiveness of existing processes and controls established to ensure ongoing compliance.

**Control effectiveness** – the determined strength of existing controls (such as training, policies and procedures, separation of duties, etc.). Control effectiveness estimates the thoroughness and strength of established controls to mitigate the risk(s) identified in each area, and takes into account the results of prior audits, examinations, compliance testing and monitoring, as well as results of the ‘controls self-assessment’ conducted by each internal Ripple department.

**Residual risk** – the perceived level of risk of non-compliance after controls have been implemented and applied.

## 6. THE POLICY

This Policy requires the Chief Compliance Officer to develop and publish a Compliance Program that includes the following components:

- A common methodology to identify and assess compliance risks;
- Testing and monitoring of controls;
- Corrective action;
- Issue escalation;
- Training; and
- Reporting.

The Compliance Program must be consistently adhered to by applicable Ripple departments.

### RISK IDENTIFICATION AND ASSESSMENT

Assessment of risk is fundamental to effective internal control and compliance risk management. Compliance conducts an annual risk assessment by first identifying all Compliance Obligations applicable to Ripple and its business activities. The



*Ripple Labs Inc. All Rights Reserved.*

Compliance team then uses the results of this risk identification to develop and update, at least annually, a “regulatory map”, indicating all regulatory requirements applicable to each internal department.

Once published, the Compliance team uses the regulatory map to work with internal departments to rate the inherent risk of each regulatory requirement in their respective areas and across Ripple.

All internal departments are required to conduct a “controls self-assessment”, evaluating the effectiveness of controls in managing applicable inherent risk in their respective areas to arrive at an overall rating reflecting perceived residual risk. Compliance provides an independent evaluation of this risk evaluation by reviewing the quality and integrity of each internal department’s self-assessment.

Note: Definitions for inherent risk, control effectiveness, and residual risk are provided in **Section 5** of this Policy.

## COMPLIANCE PLAN

The Chief Compliance Officer utilizes the annual risk assessment results to form the primary basis for priority allocation of compliance resources over the coming year to determine:

- The frequency and intensity of compliance testing;
- The type and frequency of required training; and
- Any corrective action necessary to address areas of control ineffectiveness identified in the risk assessment. Priority is given to areas of high residual risk.

The Chief Compliance Officer presents the annual Compliance Plan to the Compliance Oversight Committee for review and approval. The Committee’s primary objective is to ensure the Company complies with all Compliance Obligations. The Committee achieves this objective by overseeing the implementation of enhancements to the Compliance Policy related to program implementation, risk assessment, and issue escalation.



*Ripple Labs Inc. All Rights Reserved.*

In year one of Compliance Testing, risk assessments, control self-assessments and other reviews will be coordinated and performed simultaneously across all relevant departments. The year one review will inform the ongoing Compliance testing plan.

## **NEW PRODUCTS AND SERVICES**

New products, including significant modifications to existing products, are submitted through Ripple's New Product Risk Evaluation Process ("PREP") and are subject to approval from designated members of Ripple's Leadership Team. This process, owned by the Product Team, is separate and distinct from the annual risk assessment process outlined above. The Chief Compliance Officer, or designee, is required to evaluate the potential risks of all new products and services submitted through PREP from a compliance perspective to ensure that compliance risks are appropriately identified and can be mitigated.

## **TESTING AND MONITORING**

Ripple requires periodic and ongoing compliance testing and monitoring of activities to ensure adherence to this Policy and all applicable laws and regulations.

Broadly defined, compliance testing is performed on a selected basis according to a schedule prepared annually, or periodically under a testing program. Compliance is tested at the level of accountability. The frequency of testing activities usually ranges from six (6) to 36 months, depending on the level of risk involved. Both Compliance and internal departments are responsible for performing periodic testing of controls. Please refer to the Compliance Testing Guidelines for more information.

Monitoring includes the ongoing surveillance, review and analysis of key business performance and risk indicators carried out on an ongoing basis - daily, weekly, monthly, or can sometimes be embedded in day-to-day operations - to assist with identification of potential compliance violations. Internal department managers are responsible for the proper functioning of compliance controls in their respective areas, and perform their own monitoring and quality assurance activities. In addition, Compliance may conduct independent monitoring, as needed.



*Ripple Labs Inc. All Rights Reserved.*

Compliance develops an annual compliance testing plan, based on risk assessment results, which is presented to the Compliance Oversight Committee as part of the overall annual Compliance Plan.

The compliance testing plan establishes the schedule for testing Compliance Obligations across Ripple. The testing plan is risk-based; higher-risk regulations and policies receive more frequent testing than those with lower risk ratings. The testing plan also includes provisions for additional testing in response to unscheduled developments, such as the issuance of new rules and regulations, audit recommendations, examination findings, or internal investigations.

Any significant compliance breach or systemic weakness discovered in testing and monitoring activities is promptly escalated to the Chief Compliance Officer, or designee, who in turn escalates to the Compliance Oversight Committee and to the Board of Directors.

## **CORRECTIVE ACTION**

Internal department managers are expected to promptly address any identified compliance violations or systemic control weaknesses. Managers must consult with a member of the Compliance team and, when appropriate, the Legal department, to discuss the adequacy of corrective action and must provide agreed upon periodic status reporting to the Chief Compliance Officer, or designee.

If the initial corrective action does not satisfactorily address the issue, further action must be taken and validated by follow-up compliance testing and reporting.

The Chief Compliance Officer, or designee, is responsible for tracking, monitoring, and escalating, where necessary, the status of all corrective actions related to compliance findings.

## **ISSUE ESCALATION**

Any exceptions to this Policy should be directed to the Chief Compliance Officer, or designee, for review and advice on the potential risk arising from the exception. If the internal department chooses to accept the risk, the Chief Compliance Officer, or



*Ripple Labs Inc. All Rights Reserved.*

designee, documents this acceptance and reports it to the Compliance Oversight Committee.

If the Chief Compliance Officer believes that Ripple should not accept the risk, the case must be escalated to the Compliance Oversight Committee and, if necessary, to the Board of Directors for review and resolution. Under no circumstances will Ripple allow Policy exceptions that are likely to result in:

- Violation of law and/or regulation;
- Serious reputational harm to the Company or its affiliates;
- Material business impact or potential financial loss to Ripple in excess of \$250,000;
- Ripple or any employee becoming the subject of regulatory action or investigation.

In addition, all employees are required to escalate compliance issues, violations, or breaches either to the Chief Compliance Officer, the General Counsel, or to Ripple's confidential reporting service, accessible via phone at [REDACTED] or online at [www.ripple.ethicspoint.com](http://www.ripple.ethicspoint.com) where employee may anonymously report the matter. Any Ripple employee who, in good faith, reports an issue under this Policy is entitled to protections against retaliation, as set forth in Ripple's Code of Conduct.

## TRAINING

Compliance is responsible for developing and presenting an annual company-wide compliance training program to the Compliance Oversight Committee for approval. This program defines the compliance curriculum and identifies the frequency and appropriate audience for each training topic. The training program should be risk-based, and is designed to target any weaknesses detected through testing and monitoring activities. The program identifies the baseline training requirements for all employees as well as categories of employees that require supplementary training above the baseline level.

Following Committee approval of the program, Compliance works with the Human Resources department to execute the program. The Chief Compliance Officer



*Ripple Labs Inc. All Rights Reserved.*

provides at least an annual training update to the Compliance Oversight Committee. Records of all classes and attendance are maintained centrally by the Human Resources department and are available for review by external auditors or regulatory examiners.

## REPORTING

To ensure effective management and oversight of the Compliance Policy and Program, the Chief Compliance Officer reports at least quarterly to the Compliance Oversight Committee and periodically to the Board of Directors, as needed, on:

- Testing and monitoring results for high-risk programs;
- Material compliance issues or escalated items;
- Status of any corrective actions;
- Examination or audit findings and/or regulatory concerns;
- Upcoming regulatory examinations; and
- Emerging compliance issues that Ripple will need to address.

No less than annually, the Chief Compliance Officer submits a report on the state of compliance to assist senior management, the Compliance Oversight Committee, and the Board in evaluating any policy changes that may be appropriate.

## 7. RECORD RETENTION

Ripple's books and records are important to how it conducts business and manages employees. In addition, federal and state laws require Ripple to retain certain records, usually for specified periods of time. The accidental or intentional destruction of these records during their specified retention periods could result in consequences for Ripple and/or its employees, including:

- Fines and penalties;
- Loss of rights;



*Ripple Labs Inc. All Rights Reserved.*

- Obstruction of justice charges;
- Inference of spoliation of evidence and spoliation tort claims;
- Contempt of court charges; and
- Serious disadvantages in litigation.

Certain records must be retained because they contain information that:

- Helps satisfy legal, accounting, or other regulatory requirements;
- Serves as Ripple's corporate memory; and
- Has enduring business value (for example, evidences Ripple's rights or obligations, protects Ripple's legal interests, ensures operational continuity, is a business transaction record, etc.).

On a periodic basis, the Chief Compliance Officer, or designee, shall assess whether Ripple personnel are in compliance with recordkeeping requirements. This assessment consists of the following activities:

- Selecting a sample of records subject to Ripple's recordkeeping requirements to evaluate whether records have been maintained according to applicable policy and regulatory requirements; and
- Documenting the results of the review process and evidencing review through a written signature.

## 8. POLICY ADMINISTRATION

At least annually, Compliance will review and recommend appropriate changes to this Policy. The review may include consideration of regulatory guidelines, leadership and internal department feedback on the effectiveness of the Policy, as well as any supervisory or audit input.



*Ripple Labs Inc. All Rights Reserved.*

The Compliance Policy was last approved by the Compliance Oversight Committee and became effective on May 13, 2016.

Questions concerning this Policy should be forwarded to the Chief Compliance Officer, [REDACTED]@ripple.com.



*Ripple Labs Inc. All Rights Reserved.*



**XRP II**  
**BSA/AML/OFAC Program**  
**December 2015**

**Owner:** Chief Compliance Officer and BSA Officer I Antoinette O’Gorman | [REDACTED]@ripple.com  
**Issue Date:** September 2013  
**Last Revised Date:** December 2015



**XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

**TABLE OF CONTENTS**

<b>INTRODUCTION.....</b>	<b>3</b>
<b>SCOPE AND APPLICABILITY.....</b>	<b>3</b>
<b>POLICY STATEMENT.....</b>	<b>4</b>
DESIGNATION OF A BSA COMPLIANCE OFFICER.....	4
ROLES AND RESPONSIBILITIES.....	4
<i>BSA Compliance Officer.....</i>	<i>4</i>
<i>Compliance Oversight Committee.....</i>	<i>5</i>
<i>Company Employees.....</i>	<i>6</i>
<i>Money Transmission, Licensing and Registration.....</i>	<i>6</i>
<i>Agency Relationships.....</i>	<i>6</i>
<i>Foreign Bank Account Registration.....</i>	<i>7</i>
<i>Annual Risk Assessment.....</i>	<i>7</i>
<b>THE PROGRAM.....</b>	<b>7</b>
INTERNAL CONTROLS.....	8
<i>Customer Identification Program ("CIP") and Know Your Customer ("KYC") Activities.....</i>	<i>8</i>
<i>Identification requirements for individuals.....</i>	<i>8</i>
<i>Identification requirements for entities.....</i>	<i>8</i>
<i>Verification procedures.....</i>	<i>9</i>
<i>Prohibited Customers.....</i>	<i>10</i>
<i>Highest Risk Customers.....</i>	<i>10</i>
<i>Enhanced Due Diligence.....</i>	<i>12</i>
<b>MONITORING TRANSACTIONS FOR SUSPICIOUS ACTIVITY.....</b>	<b>12</b>
INVESTIGATIONS.....	13
REPORTING SUSPICIOUS ACTIVITY.....	14
SAR FOLLOW-UP.....	15
<i>Maintaining the Confidentiality of the SAR.....</i>	<i>15</i>
EMPLOYEE REFERRALS OF UNUSUAL ACTIVITY.....	15
ANONYMOUS REPORTING OF UNUSUAL ACTIVITY.....	16
COOPERATION WITH LAW ENFORCEMENT.....	16
NATIONAL SECURITY LETTERS ("NSLs").....	16
VOLUNTARY INFORMATION SHARING (SECTION 314(B)).....	17
<b>OFAC COMPLIANCE AND SECTION 311 SCREENING.....</b>	<b>17</b>
<b>TESTING OF CONTROLS.....</b>	<b>18</b>
INDEPENDENT AUDITING OF POLICY AND PROGRAM.....	18
<b>TRAINING AND EDUCATION.....</b>	<b>19</b>
<b>CORRECTING PROGRAM VIOLATIONS.....</b>	<b>20</b>
<b>MANAGEMENT REPORTING.....</b>	<b>20</b>
<b>RECORD KEEPING.....</b>	<b>20</b>
FUNDS TRANSMITTAL RECORDKEEPING.....	21
CURRENCY, SALE AND TRANSPORTATION OF NEGOTIABLE INSTRUMENTS.....	21
<b>POLICY VARIANCES.....</b>	<b>22</b>
<b>POLICY ADMINISTRATION.....</b>	<b>22</b>

## **XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

### **INTRODUCTION**

XRP II LLC (formerly “Fund II LLC,” “XRP II” or the “Company”), a wholly owned subsidiary of Ripple Labs, Inc., (“Ripple”) is committed to ensuring that its products and services are not used to launder money, finance terrorism, evade US government sanctions or otherwise facilitate criminal activity. It is the policy of the company to comply fully and continuously with Anti-Money Laundering (“BSA / AML”) legislation, its implementing regulations and guidance. This Policy outlines XRP II’s efforts to detect and deter money laundering and terrorist financing, and provides an overview of the major functions and responsibilities within the Company’s BSA/AML/OFAC Program.

XRP II engages in the sale and transfer of the virtual currency XRP to third parties, including individuals that are Ripple accredited investors, on a wholesale basis. XRP II makes these sales of XRP for the benefit of Ripple Labs, Inc. its ultimate parent company. Ripple Labs created and maintains the Ripple protocol, an open source, peer-to-peer payment protocol that enables free instant payments in any currency. XRP II’s sale of XRP represents one method by which Ripple raises working capital. XRP II has no other products or services and currently has no intention to develop any. Should this change at any point in the future, the BSA Officer will update the XRP II risk assessment and this document, and will implement any new or enhanced controls necessary, prior to the Company launching the new product or service.

### **SCOPE AND APPLICABILITY**

The BSA/AML/OFAC Program and Policy applies to all XRP II business activities and all XRP II personnel, as well as any service provider personnel whose activities impact the Policy and Program, are subject to compliance with prescribed requirements.

XRP II recognizes that non-compliance can expose the Company to substantial risk and civil or criminal penalties. All employees are responsible for understanding this Program/Policy and undertaking specific responsibilities assigned to them. Absent advance approval in writing from the BSA Officer, no employee, or service provider has the authority to act contrary to the provisions of this Policy or to authorize, direct, or tolerate violations of the Policy by any other person.

**Non-compliance with, or violation of, the Policy/Program’s requirements by its employees may result in:**

- **Disciplinary action, including termination in appropriate cases;  
and/or**
- **Civil and/or criminal penalties against individual employees and/or the Company itself.**

**Willful blindness, or “turning a blind eye,” to a potential money laundering violation can expose both the Company and individuals to potential liability.**

## **XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

### **POLICY STATEMENT**

XRP II will comply with the BSA and all applicable money laundering and sanctions laws and regulations in all aspects of its business. This Policy applies to all employees, Board members, and service providers whose activities relate to any aspect of the BSA program.

The Policy establishes the following four pillars of BSA/AML compliance:

- o The appointment of a qualified BSA/AML Officer ("BSA Officer");
- o The establishment of internal controls designed to limit money laundering and sanctions risks;
- o The delivery of annual BSA/AML and Office of Foreign Assets Control ("OFAC") training to employees, management, the Board and other applicable persons; and
- o The performance of independent testing of the BSA/AML and OFAC program.

### **DESIGNATION OF A BSA COMPLIANCE OFFICER**

Ripple's Chief Compliance Officer is the designated BSA Officer for XRP II, LLC BSA Officer and is responsible for directing, implementing, enforcing, maintaining, and updating the Company BSA/AML/OFAC Policy and Program. The BSA Officer reports directly to Ripple, Inc.'s Chief Operations Officer with an independent dotted reporting line to the Ripple Board of Directors.

The BSA Officer and her employees have the authority to access all company records and direct all company personnel as necessary to implement this Policy and Program.

### **ROLES AND RESPONSIBILITIES**

Below is a brief description of the roles and responsibilities of various functions within XRP II with respect to BSA/AML/OFAC compliance.

#### **BSA Compliance Officer**

BSA Officer responsibilities include:

- o Implementing and maintaining the BSA/AML/OFAC Program and Policy, and related procedures;
- o Providing quarterly reporting to XRP II's Compliance Oversight Committee evidencing appropriate governance of XRP II's BSA/AML/OFAC compliance program
- o Reviewing and refreshing the BSA/AML/OFAC Program and Policy, procedures, risk assessment, and any relevant training materials at least annually, or more frequently as circumstances require;
- o Maintaining training records as they relate to BSA/AML and OFAC training for XRP II staff;
- o Reporting to Treasury and managing XRP II's response to potential OFAC hits;
- o Overseeing execution of the Program, including KYC and suspicious activity monitoring/reporting activity, providing guidance and direction to XRP II staff on effective Program implementation;
- o Ensuring that the Company adheres to timely AML and sanctions reporting, including designing appropriate controls and coordinating independent testing of their effectiveness;

## **XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

- o Ensuring that all staff are knowledgeable regarding potential red flags and is aware of their responsibility to promptly report violations or potential suspicious activity through the escalation procedures described in this Program;
- o Reviewing any changes to AML and sanctions laws, regulations, guidance in consultation with regulatory advisors and outside counsel to ensure that the Company remains fully compliant with legal obligations and or regulatory expectations;
- o Promptly alerting the Compliance Oversight Committee and executive management to any material issues of BSA/AML/OFAC non-compliance, and instituting and monitoring corrective action;
- o Maintaining appropriate MSB registration and pursuing required money transmitter state licenses;
- o Projecting and implementing resource plans to ensure the Program can be effectively executed;
- o Conducting periodic monitoring/quality assurance of BSA controls;
- o Periodically validating monitoring systems and parameters;
- o Evaluating any new products and services for BSA/AML and OFAC risk and ensuring that XRP II has sufficient controls in place to mitigate its risk prior to launch;
- o Coordinating and ensuring that independent program testing takes place at least annually.

The BSA Officer is further responsible for:

- o Presenting an BSA/AML/OFAC Program and corresponding risk assessment, as well as the BSA/AML/OFAC training Program to XRP II's Compliance Oversight Committee for review and approval on a no less than annual basis;
- o Reporting to Ripple' Board of Directors annually on the approval of the BSA/AML/OFAC Program, the corresponding risk assessment, and all relevant BSA/AML/OFAC training materials by XRP II's Compliance Oversight Committee;
- o Providing semi-annual reporting to the Ripple Board of Directors evidencing appropriate governance of the XRP II's BSA/AML/OFAC Compliance Program;
- o Providing BSA/AML/OFAC training to the Ripple Board of Directors and Compliance Oversight Committee members on an annual basis, or more frequently, as needed; and
- o Ongoing consultation with regulatory advisors and legal counsel to ensure that XRP II's BSA/AML/OFAC Program remains current with applicable laws and leading industry standards.

XRP II has also designated a qualified BSA Manager and BSA Investigations Manager, reporting directly to the BSA Officer, to support compliance with all aspects of XRP II's BSA Program requirements.

### **Compliance Oversight Committee**

As of November 2016, XRP II's Program is governed by a Compliance Oversight Committee that meets quarterly, or more frequently as needed. The Oversight Committee comprises the BSA Officer, Ripple's General Counsel, and Ripple's Head of Regulatory Relations and Strategic Policy Initiatives. The Committee reports no less than semi-annually to the Ripple Board of Directors. The Compliance Oversight Committee also maintains responsibility for oversight of necessary remediation of and enhancement to the BSA/AML/OFAC Program, which can include self-identified issues as well as issues arising from independent testing or examinations.

The Compliance Oversight Committee is responsible for:

- o Promoting and implementing a strong culture of compliance;
- o Ensuring that the Company appoints a suitably qualified BSA Officer with appropriate levels of staffing support;
- o Overseeing the BSA Officer (the BSA Officer will recuse herself from this responsibility);
- o No less than annually, approving this Policy, the BSA/AML/OFAC risk assessment and the BSA/AML/OFAC Training Program;

## **XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

- o Establishing and communicating an appropriate risk tolerance for BSA/AML and OFAC risk;
- o Reviewing compliance reports and any compliance issues escalated to executive management, including mitigation plans;
- o Periodically reviewing the adequacy of compliance resources;
- o Reviewing periodic BSA/AML/OFAC compliance reports from the BSA Officer; and
- o Reviewing the results of independent testing and examinations, ensuring that XRP II takes appropriate action to remediate or enhance its BSA Program taken, where indicated.

### **Company Employees**

All Company employees are fully accountable for:

- Reviewing and understanding the BSA/AML/OFAC Program;
- Escalating any unusual or potentially suspicious activity that they observe or detect in the normal course of business, to the BSA Officer, either through the designated escalation procedures;
- Attending required AML training in accordance with XRP II's BSA/AML/OFAC Training and Education Program;
- Escalating actual or potential compliance weaknesses to the BSA Officer, and working with the BSA Officer to implement corrective action as needed;
- Maintaining systems, controls, and reports that support BSA/AML and sanctions compliance efforts as directed by the BSA Officer;
- As applicable, notifying and seeking the BSA Officer's approval for new or modified products or services; and
- Otherwise assisting and complying with requirements of XRP II's BSA/AML/OFAC Program and policy, as needed.

### **Money Transmission, Licensing and Registration**

The BSA Officer is responsible for XRP II's registration as a money services business with FinCEN and maintains the Company's federal registration and renewal as required by law. XRP II last renewed its registration with FinCEN in December 2014. The BSA Officer maintains responsibility for monitoring and initiating state license applications, where needed. The Company retains all documents regarding MSB or other money transmitter registration and state licensure indefinitely.

XRP II was organized in South Carolina, a state in which MSBs are not currently subject to money transmitter licensure requirements. Consequently, the BSA Officer, in consultation with legal counsel, has determined that the Company is not subject to state licensing as a result of its virtual currency activities, except in the state of New York.

### **Agency Relationships**

The Company does not have agents and will not establish any agency relationships. Should XRP II decide to use agents at any time in the future, the Company shall establish and implement appropriate controls to comply with MSB agent requirements, including but not limited to the creation of a list of such agents and development of effective agent oversight mechanisms, in advance of pursuing the agency relationships.

## **XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

### **Foreign Bank Account Registration**

XRP II does not maintain a foreign bank account and therefore has no FBAR filing obligation. Should XRP II decide at any time in the future to open and maintain a foreign bank account, the Company will establish controls to comply with FBAR reporting requirements in advance of opening the account.

### **Annual Risk Assessment**

The BSA/AML/OFAC risk assessment identifies XRP II's risks and assesses controls the Company has implemented to meet the regulatory expectations for money service businesses. The BSA Officer or appointed designee conducts the risk assessment process including:

- Rating the inherent risk of XRP II's products and services, its customer base and the geographies in which its customers are located;
- Identifying and assessing the adequacy of XRP II controls in light of the BSA/AML and OFAC requirements for money transmitters registered with FinCEN;
- Rating the Company's residual risk in consideration of assessed controls; and
- Identifying and assigning responsibility for any necessary control enhancements identified as a result of the risk assessment process.

The BSA Officer or appointed designee updates the Company's risk assessment on an annual basis. The updated risk assessment is presented annually by the BSA Officer to XRP II's the Compliance Oversight Committee for review and approval. Additionally, the BSA Officer is responsible for presenting and reporting this approval to the Ripple Board of Directors.

The purpose of the risk assessment is to identify XRP II's BSA/AML and OFAC risks, and assess controls XRP II has implemented to meet the regulatory expectations for an MSB. The risk assessment forms the basis of the annual BSA/AML/OFAC Program, and will:

- Identify the Company's risk profile, by assessing the inherent risks presented by XRP II's products and services, customer base and the geographies in which it or its customers operate;
- Determine the adequacy and effectiveness of Company's controls;
- Identify the existence of any insufficiently mitigated risk; and
- Recommend any necessary enhancements to the BSA/AML/OFAC Compliance Program needed to reduce residual risk to an acceptable level. From time to time, as part of the risk assessment process, the BSA Officer may recommend particular leading practice enhancements for certain BSA/AML/OFAC controls, as deemed appropriate.

### **THE PROGRAM**

An effective BSA/AML/OFAC Program is essential to both achieving and demonstrating compliance with legal requirements. This BSA/AML/OFAC Program is updated on an annual basis, or more frequently should circumstances warrant, and is presented annually by the BSA Officer to the Compliance Oversight Committee for review and approval. An overview of the Program is as follows:

## **XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

### **INTERNAL CONTROLS**

#### **Customer Identification Program ("CIP") and Know Your Customer ("KYC") Activities**

The Company employs customer identification procedures to verify the identities of our customers, screens customer and associated party names to ensure that they are not subject to OFAC sanctions, and conducts appropriate customer due diligence, including obtaining expected transaction activity, source of funds information as well as information regarding products and services offered by the customer.

The BSA Officer, or designee, reviews all potential customers prior to onboarding and rejects customers that the company cannot adequately verify are subject to OFAC sanctions, or otherwise pose unacceptable BSA/AML risks.

XRP II carries out its CIP and KYC programs as follows: XRP II collects customer identification information and verifies that information before permitting a customer to conduct an initial transaction, and on an ongoing basis as necessary or required by law. Due to the high inherent BSA/AML risk associated with virtual currency, the Company conducts additional due diligence on all of its customers. The Company also conducts the following screenings on all direct XRP II customers; where the direct customer of XRP II is an entity, XRP II also conducts full screening on all 25% or more beneficial owners, as follows: OFAC sanctions screening; politically exposed person ("PEP") screening; and, negative news, and a general internet searches for other potential risk factors.

Compliance personnel working under the direction of the BSA Officer undertake the KYC process. Completed KYC forms are required for each direct customer of XRP II, be that an individual or an entity. However, if a beneficial owner of an entity is identified as a PEP, in addition to requiring a KYC form to be completed by the entity, a KYC form must also be completed by the identified PEP.

#### **Identification requirements for individuals**

To purchase XRP from the Company, an individual must provide:

- Full legal name;
- Physical Address;
- Date of Birth;
- Tax payer identification number (TIN) such as a social security number or other government-issued identification number acceptable to the BSA Officer; and
- Copy of a valid, government-issued photo identification card such as a driver's license or passport
- Copy of a photograph of the individual holding their ID such that the person's face and picture on the ID are visible to the camera

#### **Identification requirements for entities**

To purchase XRP from the Company, an entity must provide:

- Full legal name of the entity;
- Physical business address;

## **XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

- Taxpayer Identification Number (TIN);
- A list of all beneficial owners or ultimate beneficial owners with 25% or more ownership;
- Copy of a document evidencing the legal existence of the entity, such as articles of incorporation or association<sup>1</sup>;
- Copy of a photograph of all persons with 25% or more beneficial ownership holding their ID visible to the camera;
- Proof of address or existence of physical location of the entity.

### **Verification procedures**

The BSA Officer, or designee, review for inconsistencies in the information provided by the customer, and considers documentary evidence, non-documentary evidence or both to verify a customer's identity.

In the first instance, the BSA Officer or designee, make use of available documentary evidence to verify customer identity. Compliance personnel may also use non-documentary means such as online verification services to verify customer identity if:

- (1) Compliance personnel are unfamiliar with any documents presented; or,
- (2) the BSA Officer or designee believes it will provide greater assurance about the identity of the customer.

The Company will not conduct business with a customer who does not provide identification information. If a potential or existing customer refuses to provide all requested CIP and KYC information or appears to have intentionally provided misleading information, the Company will not conduct any further transactions with the customer. In such circumstances, the BSA Officer will determine whether to file a SAR.

If the Company cannot verify the true identity of a potential customer to the satisfaction of the BSA Officer, she will:

- Ensure that Company does not conduct any transactions with that individual or entity, or otherwise establish a customer relationship; and
- Determine whether to file a SAR.

The Company documents its customer identification and verification, including all identifying information, the methods used and results, and the resolution of any discrepancies. The Company will keep records containing a description of any document relied on to verify a customer's identity, noting the type of document, any identification number in the document, the place of issuance, and if any, the dates of issuance and expiration. With respect to non-documentary verification, the Company will retain documents that describe the methods and the results of any measures it took to conduct such verification.

---

<sup>1</sup>

For all articles of incorporation and identity verification documentation presented that is not in English, it is the responsibility of the customer to provide a third party translation. With the exception of proof of address, which may be a utility bill, lease agreement, or other document with the customer's name and address, XRP II will not accept documentation in a language other than English.

**XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

XRP II will retain records of required identification obtained at account opening for the duration of the customer relationship and for five (5) years after the customer account is closed (or five (5) years after the last transaction undertaken by the customer).

**Prohibited Customers**

XRP II will not support activity of entities prohibited by law or regulation such as:

- o entities that issue bearer shares;
- o any OFAC-sanctioned persons;
- o unauthorized on-line gambling companies;
- o shell banks;
- o shell companies<sup>2</sup>;
- o unlicensed or unregulated financial institutions<sup>3</sup>;
- o persons featured on Section 311 Special Measures lists; and
- o any individual or entity undertaking, or with close ties to, activity contrary to U.S. law or regulation.

In addition, XRP II will not onboard a customer relationship of any individual or entity the BSA Officer determines presents unacceptable AML or sanctions risks to the Company. This includes, but is not limited to, persons identified with prior convictions for financial-related crimes that indicate unacceptable risks of money laundering, terrorist financing and/or sanctions evasion.

The Company will prevent prohibited entities from becoming customers or otherwise accessing XRP II. Should prohibited entities be identified through CIP/KYC efforts, they must be immediately escalated to the BSA Officer for review, investigation, escalation to senior management, and ultimate termination.

**Highest Risk Customers**

XRP II subjects all higher-risk customers to EDD according to the standards set down in the next section.

***1. Politically Exposed Persons (PEPs)***


---

<sup>2</sup> The term "shell company," refers to non-publicly traded corporations, limited liability companies (LLCs), and trusts that typically have no physical presence (other than a mailing address) and generate little to no independent economic value. Most shell companies are formed by individuals and businesses for legitimate purposes, such as to hold stock or intangible assets of another business entity or to facilitate domestic and cross-border currency and asset transfers and corporate mergers. Shell companies have become increasingly common tools for money laundering and other financial crimes, primarily because they are easy and inexpensive to form and operate. Because shell companies can obscure company structure, ownership, and activities, XRP II considers them to be prohibited customers. Shell companies that issue bearer shares are also prohibited from conducting business with XRP II.

<sup>3</sup> Except when licensing is not required in country of incorporation

**XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

When evaluating potential XRP II customers, the BSA Officer, or appointed designee, conducts comprehensive screening to determine whether the potential customer is a known PEP. PEPs are generally defined as:

- A “**senior foreign political figure**” is a senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned corporation. In addition, a senior foreign political figure includes any corporation, business, or other entity that has been formed by, or for the benefit of, a senior foreign political figure.
- The “**immediate family**” of a senior foreign political figure typically includes the figure’s parents, siblings, spouse, children, and in-laws.
- A “**close associate**” of a senior foreign political figure is a person who is widely and publicly known to maintain an unusually close relationship with the senior foreign political figure, and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of the senior foreign political figure.

XRP II considers all PEPs to be high risk and subject to annual compliance reviews. Upon identification of a PEP, in addition to requiring and obtaining a completed KYC form, designated XRP II compliance staff will request and review information concerning:

- the potential customer’s background, income sources, source of funds and wealth and any other financial information deemed appropriate;
- the purpose of the account(s) and expected volume and nature of account activity;
- details of any immediate family members or close associates with transaction authority over the account or benefitting from transactions conducted through the account.

All identified PEPs, whether a direct customer or associated parties (25% or more beneficial owners) of a direct customer of XRP II, require BSA Officer approval prior to onboarding. Customers identified as PEPs cannot conduct transactions with XRP II until such time all requested documentation has been received, reviewed and approved by the BSA Officer. The Company will not conduct business with any PEP, or PEP associated entity, who does not provide, or refuses to provide, KYC and other requested information. In such circumstances, the BSA Officer will determine whether or not the filing of a SAR is warranted.

Identified PEPs will be coded as such in the ‘Annotations’ database for reporting, tracking, and targeted transaction monitoring purposes. The Annotations database is an internal system managed by a central Ripple administrator for recording additional information about XRP II customers.

At this time, XRP II has identified no PEP customers or associated parties. If an existing customer or associated party is subsequently identified as a PEP, through ongoing PEP screening of active<sup>4</sup> customers and associated parties, all relevant risks will be evaluated and appropriate action taken at that time.

## ***2. Customers Named in Multiple Reported Instances of Suspicious Activity***

Any XRP II customer named as the subject of one (1) or more suspicious activity reports (SARs) filed with FinCEN will be subjected to EDD. Instances of three (3) or more SAR filings require escalation to the Compliance Oversight Committee for retention or termination decision.

<sup>4</sup> An ‘active’ customer is defined as one that has conducted any transaction within the prior rolling six month period.

## **XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

Additional factors determining consideration for risk-based EDD include, but are not limited to:

- o transaction activity levels equivalent to USD equivalent of \$500,000 total incoming or outgoing transactions in any one month;
- o customers with Ripple balances above \$500,000; and
- o geographic location.

---

### **Enhanced Due Diligence**

XRP II conducts EDD on all highest-risk customers, as defined in the previous section. This EDD will include:

- o Negative news and internet searches;
- o Collection and analysis of information on source of funds and/or purpose of transactions;
- o Assessment of expected transactional activity; and
- o (For existing customers) Review of actual transactional activity against expected activity and other known facts about the customer.

XRP II will perform annual reviews on active customers that remain above EDD transaction thresholds. In addition, the BSA Officer will close any accounts where due diligence measures cannot be applied or EDD reveals unacceptable levels of money-laundering, terrorist-financing or sanctions risks.

### **MONITORING TRANSACTIONS FOR SUSPICIOUS ACTIVITY**

The Company monitors its services for suspicious activity and reports this activity as required by law. In addition to filing suspicious activity reports ("SARs"), law enforcement is notified of any cases that specific agencies may have particular interest in. The Company and its employees will not engage in activities that would facilitate any form of suspicious activity through willful blindness, by actively structuring transactions to evade reporting requirements, or hiding the identity of customers.

XRP II monitors all customer transactions for suspicious activity. Suspicious activity is activity that indicates the possibility of:

- o Transactions and patterns of transactions involving illegal XRP's,
- o Transactions designed to evade the BSA and its regulations,
- o Transactions that serve no business or lawful purpose, and
- o Transactions that appear to attempt to use the Company to facilitate criminal activity.

Due to the wholesale nature of its business and the relatively small number of transactions, all of XRP II's transactions are individually reviewed by the BSA Investigations Team. When warranted, this review can include assessment of the totality of transactions conducted by that customer and consistency of those transactions with the KYC information collected.

**XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

In conducting transaction monitoring, the BSA Investigations Team look for “red flags” that could indicate possible suspicious activity. Such red flags include, but are not limited to:

- A customer uses a false ID, or multiple IDs on different occasions (name, address, or identification number may be different);
- Two or more customers use the same or similar IDs;
- A customer breaks a large transaction into two or more smaller transactions to avoid transaction limits or reporting requirements;
- A large transaction is broken into two or more smaller transactions conducted by two or more people;
- The amount of the transaction is unusually large or otherwise unusual for the customer;
- The customer makes the same or similar transactions more frequently than normal;
- The customer conducts transactions so they fall just below monetary amounts that require reporting or recordkeeping;
- Two or more customers seem to be working together to break one transaction into two or more transactions;
- A customer uses two or more Company accounts or funding agents on the same day to break a transaction into smaller ones;
- A customer exhibits unusual concern about the Company's government reporting practices and BSA/AML policies;
- A customer engages in a transaction lacking business sense or inconsistent with his or her stated business;
- KYC information provided by a customer (e.g. in relation to source of funds) is false, misleading, or substantially incorrect;
- Upon request, a customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets;
- A customer (or a person publicly associated with one) has a questionable background, or is the subject of news reports indicating possible criminal, civil, or regulatory violations;
- A customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate reasons, to provide information regarding that person or entity;
- A customer cannot describe his or her business;
- A customer is from, or has accounts in, a non-cooperative territory identified by the Financial Action Task Force (FATF);
- A customer requests that a transaction be processed in a manner that avoids Company's normal documentation requirements; or
- A customer has inflows of funds or other assets beyond their known income or resources.

**Investigations**

Should Compliance staff identify, or be notified of, suspicious activity or a red flag, the BSA Investigations Manager, under the direction of the BSA Officer, will initiate an investigation into the activity. All steps conducted during this investigation must be documented. If it is determined that the activity in question is not suspicious, the reasoning behind this decision must be clearly documented and recorded in the investigation file.

**XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

**Reporting Suspicious Activity**

The BSA Officer, or appointed designee, will initiate the filing of a SAR if the amount of suspicious activity identified is over USD \$2,000<sup>5</sup> and:

- involves funds from illegal activity, or was conducted to hide or disguise funds or assets or funds from illegal activity (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation, or to avoid any transaction reporting requirement under federal law or regulation;
- is designed to evade any requirement of the BSA or related regulations;
- serves no business or apparent lawful purpose, and the Company knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction;
- involves using the Company to facilitate criminal activity;
- incidents of unauthorized electronic intrusion into the Company's computer system to:
  - remove, steal, procure, or otherwise affect funds of the Company or the Company's customers;
  - remove, steal, procure, or otherwise affect critical information including customer account information; or
  - damage, disable, or otherwise affect critical systems of the Company.

The BSA Officer, or designee, may choose to report the suspicious activity voluntarily if the transaction falls below the USD \$2,000 monetary threshold in cases where a SAR may provide useful information to law enforcement. The BSA Investigations Manager, under the direction of the BSA Officer is responsible for the final determination regarding whether a report is required or will be voluntarily made and is responsible for ensuring that the SAR is filed no later than 30 days after the determination that suspicious activity has occurred.

If the potential violation requires immediate attention, such as in the case of ongoing money laundering, the BSA Officer or appointed designee will immediately notify by telephone the appropriate law enforcement agency, in addition to filing a SAR. Moreover, should the activity in question indicate the possibility of terrorist activity, the BSA Officer or appointed designee will voluntarily report the activity to FinCEN, as appropriate.

Should the BSA Officer or designee determine that any of the following conduct is occurring, Federal law enforcement will be immediately notified by telephone:

- A customer account holder, or a person with whom such an account holder is engaged in a transaction, is listed on or located in a country or region listed on the OFAC list;
- A customer account is held by an entity that is owned or controlled by a person or entity listed on the OFAC list;
- A customer tries to use bribery, coercion, or similar means to open an account or carry out a suspicious activity;
- The Company has reason to believe a customer is trying to move illicit cash out of the government's reach;

<sup>5</sup> Potential criminal violations involving insider abuse will be reported notwithstanding the dollar amount involved.

## **XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

- o The Company has reason to believe a customer is about to use the funds to further an act of terrorism, engage in money laundering, or otherwise engage in illegal activity; or
- o The Company has other reasons to believe that one or more law enforcement agencies may benefit from direct notification of the suspicious activity.

### **SAR Follow-up**

In the event that a SAR is filed, the BSA Officer will determine whether it is appropriate to terminate the customer relationship in question. This determination will be reached using a risk-based approach, taking into account the nature and location of the customer, the volume and size of the customer's transactions, and other relevant factors affecting the risk profile of the customer. The BSA Officer or appointed designee is responsible for documenting the basis for the decision reached. When the customer relationship is not terminated, the BSA Officer, or designee, will conduct a follow-up 90-day review to determine whether there is continuing activity that warrants an additional SAR filing.

All instances of three (3) SARs filed on any customer relationship requires automatic escalation by the BSA Officer to the Compliance Oversight Committee for customer termination/retention decisioning.

Copies of all SARs filed and all supporting documents must be retained securely and confidentially for at least five (5) years after filing.

### **Maintaining the Confidentiality of the SAR**

No officer, director, employee, agent, or service provider of Company may notify any person outside of the Company that any transaction or person has been reported in a SAR.

The Company prohibits all staff from "tipping off" users that they are under investigation or that Ripple has filed a SAR naming them. The BSA Officer ensures that all employees receive training (including the prohibition against "tipping-off") on how to report suspicious activity as part of the BSA/AML/OFAC training program, which is summarized below. To reduce risk of disclosure, the Company restricts internal access to SAR filings, documentation and other SAR-related information to the BSA Officer, Compliance staff and executive management.

### **Employee Referrals of Unusual Activity**

To facilitate internal reporting of unusual behavior or activity, the Company has established an internal Unusual Activity Reporting ('UAR') process governing the escalation, receipt, and processing of employee reports of unusual activity or suspected non-compliance with XRP II's BSA/AML/OFAC Program. While employees should not attempt an investigation themselves before escalating, to the extent possible, referrals to Compliance should include any identifying information on the party in question, details of the related activity, information regarding additional parties to the transaction and the basis for suspecting potential illegal activity.

Only designated Compliance staff members have access to UARs submitted by Company employees.

## **XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

Reports of all incoming escalations and their ultimate resolution are maintained securely for a period of five (5) years from the date of employee submission (or from the date of SAR filing, if warranted).

### **Anonymous Reporting of Unusual Activity**

Should a Company employee wish to anonymously report unusual or potentially suspicious activity, or non-compliance with this BSA/AML/OFAC Program, he or she may do so using the Company's confidential reporting service, accessible via phone at [REDACTED] or online at [www.ripple.ethicspoint.com](http://www.ripple.ethicspoint.com).

Designated Compliance staff have direct access to the anonymous online e-mail inbox and voicemail and are responsible for maintaining strict confidentiality of reported information, disclosing only suspected activity and not the name of the individual who submitted the report, and only as necessary to implement the BSA/AML/OFAC Program.

Reports of all incoming escalations and their ultimate resolution are maintained securely for a period of five (5) years from the date of employee submission.

### **Cooperation with Law Enforcement**

It is Company policy to cooperate to the extent permitted by applicable law and in accordance with its policies, with legal process or other requests for information or assistance received from law enforcement in accordance with established internal procedures governing responses to law enforcement requests.

The BSA Officer reviews all subpoenas and requests for information or assistance from law enforcement, consults with legal counsel prior to disclosing any information to determine whether it is permissible to provide the requested information or assistance, and then responds accordingly to law enforcement.

Records of law enforcement legal process and requests, and productions made in response will be retained for five (5) years.

Confidential records of law enforcement requests and productions are maintained and disclosed only:

- o as allowed by legal process;
- o within the Company or to outside counsel as necessary to comply with the request;
- o for legal advice; or
- o to prepare a responsive production.
- o

### **National Security Letters ("NSLs")**

Upon receipt, NSLs must be referred to the BSA Officer who consults with legal counsel prior to disclosure of any information. NSLs must be treated with the highest levels of confidentiality; the existence of a NSL will be disclosed only as necessary to comply with the requests contained in it. NSL records must be

## **XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

maintained confidentially and securely. The BSA Officer is responsible for responding to all law enforcement requests. Records of NSLs and responsive documents are retained for a period of five (5) years.

### **Voluntary Information Sharing (Section 314(b))**

The Company has notified FinCEN that XRP II elects to share information pursuant to section 314(b) of the USA Patriot Act. The BSA Officer, or appointed designee, will renew the notice on an annual basis, as appropriate. Before undertaking any voluntary information sharing, the BSA Officer, or designee, must ensure that if the information is to be shared with the financial institution, that financial institution has filed the appropriate notice with FinCEN.

The BSA Officer, or designee, is responsible for handling and tracking all incoming 314(b) requests in accordance with established 314(b) procedures, as well as drafting and approving all outgoing 314(b) requests. The BSA Officer or designee will ensure that all outgoing requests are limited exclusively to investigations of possible money laundering or terrorist financing and will ensure that the information is used only for the following purposes:

- o Identifying and, where appropriate, reporting on money laundering or terrorist activities;
- o Determining whether to establish or maintain an account, or to engage in a transaction; or
- o Assisting the sharing financial institution in complying with performing such activities.

If shared information reveals potential suspicious activity occurring through XRP II, the BSA Investigations Manager, under the direction of the BSA Officer, will initiate an investigation, which may result in the filing of a SAR in accordance with this Policy.

Records of information shared and information received will be retained for five (5) years. Any such records must be maintained confidentially and securely.

### **OFAC COMPLIANCE AND SECTION 311 SCREENING**

The Company screens all customers, both individual and entities and their associated parties, as well as all XRP II employees, against the OFAC SDN list prior to onboarding. The Company screens new customers and associated parties against OFAC's SDN list and jurisdictions subject to broad OFAC sanctions, as well as list of special measure entities, jurisdictions and transactions provided by FinCEN. The Company will not conduct any transactions, or otherwise establish a customer relationship, with any individuals or entities subject to OFAC sanctions.

All active customers and associated parties of active customers are automatically rescreened on a daily basis. For existing customers, the BSA Officer designee, must approve each time a customer transacts, unless the transaction is within one month of a previous transaction or is consistent with past customer activity. Designated compliance staff review all XRP II transactions on a quarterly basis to confirm/validate this activity.

No staff member will conduct any transactions with any individual or entity under review for possible OFAC matches.

## **XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

All potential OFAC matches must be referred to the BSA Officer for review, except in circumstances where procedures specifically authorize other staff to resolve obvious false positives. Should the Company determine that a customer or someone with or for whom the customer is transacting is named on an OFAC or other prohibited list, or is from or engaging in transactions with a person or entity in a prohibited country or region, the BSA Officer, will take appropriate steps to block the assets in question and will file a blocked assets or rejected transaction form with OFAC. The Company has implemented controls to block IP addresses from countries with broad OFAC sanctions programs to ensure that any person utilizing these IP addresses cannot access Ripple or XRP II's services.

All true OFAC matches must be reported by the BSA Officer to OFAC, in writing, within ten (10) business days of identification and are also reported to the Compliance Oversight Committee and executive management, as identified. The BSA Officer or designee, will report blocked or rejected transactions on the Ripple protocol to OFAC within ten (10) business days and may also call the OFAC Hotline at 1-800-540-6322 to report the activity. The BSA Officer, or designee, is also responsible for reporting all blocked property as of June 30 by September 30 on an annual basis. The annual report must reflect all blocked property (accounts, specific transactions, etc.) held by XRP II as of June 30 in the given reporting year. All blocked assets must be maintained in interest-bearing accounts.

The Company must retain records of transactions subject to OFAC screening for a minimum of five (5) years.

### **TESTING OF CONTROLS**

#### **Independent Auditing of Policy and Program**

In addition to conducting routine internal and overseeing annual execution of external independent testing of the BSA/AML OFAC Program, the BSA Officer, or designated Compliance staff, is responsible for:

- o assessing the risk posed by any new products that XRP II offers and for ensuring that the Company has developed implementing controls prior to launch; and
- o effective risk-based due diligence and oversight of critical third-party providers that operate, assist with, or provide support for any of XRP II's controls for BSA/AML/OFAC processes.

In addition to conducting routine internal testing, the BSA Officer regularly consults with our regulatory advisors and legal counsel to ensure that our BSA/AML/OFAC Policy and Program stays current with applicable laws and leading industry standards.

The BSA Officer will identify a qualified, independent third party to conduct testing of the Company's BSA/AML/OFAC controls on an annual basis.

Annual testing will include an audit of Company's compliance with its own BSA/AML/OFAC Program. The audit must include, at a minimum:

- o Evaluation of the overall integrity and effectiveness of Company's BSA/AML Program;
- o Testing of all affected areas to ensure compliance with the BSA/AML Program;
- o Reviewing the flow of funds and the scope of Company's business to determine whether additional compliance controls should be added to the BSA/AML/OFAC Program;

## **XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

- o Reviewing exception items to the BSA/AML/OFAC Program;
- o Reviewing the process for referring, investigating and reporting suspicious activity and “red flags”;
- o Sampling of transactions for compliance, with an emphasis on high- risk transactions;
- o Reviewing and testing compliance for recordkeeping and record retention policies;
- o Reviewing and testing procedures for OFAC screening and customer and identification and verification (KYC);
- o Evaluating the Company’s response to any previously identified deficiencies;
- o Reviewing adequacy of the training program; and
- o Reviewing of Program controls.

The auditor will issue a report of its findings upon completion of its audit directly to executive management; this report of findings should not be routed through the Compliance function. The report must include any deficiencies and recommendations for enhanced compliance, including any recommended changes to the BSA/AML/OFAC Policies or Program. The BSA Officer will create and implement a remediation plan to address each of the resulting recommendations, as appropriate.

Records of independent testing must be retained for at least five (5) years.

### **TRAINING AND EDUCATION**

The BSA Officer or appointed designee is responsible for ensuring that employees receive appropriate training on the requirements of the Company’s BSA/AML/OFAC Policy and Program. The BSA Officer is responsible for providing BSA/AML/OFAC training to the Ripple Board of Directors on an annual basis, or more frequently if needed.

All relevant training materials must be approved annually by the Compliance Oversight Committee. Evidence of this approval is then reported annually to the Ripple Board of Directors by the BSA Officer. Records of approvals are maintained centrally by the XRP II Compliance team.

Training will include a review of this BSA/AML/OFAC Policy and program, as well as a discussion of the following, with sufficient detail to allow each person receiving the training to perform his or her job function:

- o The Company’s responsibilities for compliance under the BSA, the USA PATRIOT Act, the OFAC statutes and regulations, and any other applicable laws, including specific program controls;
- o Designated roles in the BSA/AML/OFAC Program;
- o The function and of the BSA Officer;
- o Any recent changes to regulations or internal processes and controls;
- o How to identify red flags and signs of suspicious activity and what to do when risks are identified;
- o The Company’s record-keeping and document retention policies; and
- o Consequences to the Company and to individuals for non-compliance, including statutory penalties and internal discipline/penalties.

## **XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

Trainees must receive initial training within thirty (30) days of joining the Company, where feasible, and at least annually thereafter, /or more frequently when significant changes to the laws governing the BSA/AML/OFAC Program warrant.

The BSA Officer, or designated compliance staff, is responsible for retaining records for at least five (5) years from the date of training for each trainee.

### **CORRECTING PROGRAM VIOLATIONS**

The BSA Officer will take appropriate measures to correct any violations of this BSA/AML/OFAC Program. Regarding internal violations of the Program, the BSA Officer will consult with appropriate personnel within the Company to ensure that appropriate corrective action is taken in accordance with the applicable employment or other internal Company policy(ies).

With respect to violations of the BSA/AML/OFAC Program by external service providers, agents or subcontractors, the BSA Officer will consult with the appropriate Company business and legal personnel to take appropriate action in accordance with the applicable agreement with the entity.

Records of corrective action shall be retained for at least five (5) years, or longer if required by the laws implicated in the corrective action (for example, by employment or contract law).

### **MANAGEMENT REPORTING**

The BSA Officer prepares quarterly compliance reports for the Compliance Oversight Committee and semi-annual reporting to the Board of Directors of XRP II's parent company, Ripple, Inc. This report describes key Program activities and reports on key risk indicators such as identified instances of suspicious activity, fraud or other wrongdoing. Reporting must evidence appropriate and comprehensive governance of XRP II's AML Program.

Quarterly BSA Compliance reporting to the Compliance Committee may include:

- regulatory compliance and MSB updates related to Virtual Currency;
- recent global money laundering enforcement actions;
- state regulatory reporting and licensing updates;
- notification and/or results of examinations and audit reviews;
- training, compliance staffing, and technology resource needs;
- statistics on numbers of SARs filed;
- bank relationship status; and,
- any other relevant required regulatory reports.

### **RECORD KEEPING**

The Bank Secrecy Act ("BSA") establishes recordkeeping requirements related to various types of records, including customer accounts, and may impose other filing requirements needed to document a financial institution's overall compliance with the BSA. In general, the BSA requires financial institutions to

## **XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

maintain most records for at least five years. Records can be maintained in many forms including original, electronic, copy, or a reproduction. XRP II is not required to keep a separate system of records for each BSA requirement; however, it must maintain all records in a way that makes them accessible within a reasonable period of time.

The Company maintains records of customer identity, verification on a dedicated secure Compliance server accessibly solely by members of the Compliance team. Due diligence and suspicious activity investigations and reports, as well as disclosures of information in response to governmental requests are maintained by Compliance. Additional records, as required by law, are also created and maintained by Compliance. This Program requires retention of all records for a minimum of five years, as well as retention of customer records for a minimum period of five years after the end of the customer relationship.

### **Funds Transmittal Recordkeeping**

With respect to any single transaction or aggregated series of transactions from one individual or multiple individuals known to be acting in concert totaling more than USD \$3,000 in a single day, the Company will collect and retain the following records:

- The name and address of the customer;
- The amount of the order;
- The execution date of the order;
- Any payment instructions received from the customer;
- As many of the following received with the order: the name and address of the recipient, the account number of the recipient, or any other specific identifier of the recipient; and
- Any form relating to the order that is completed or signed by the customer placing the order.

When the Company is the transmitter of a transmittal order of USD \$3,000, it provides to the customer, at the time it sends the order to the receiving destination, the following information:

- The amount of the order;
- The execution date of the order;
- The identity of the recipient's Ripple wallet; and
- Any other information deemed relevant to the order.

The Company retains the records of subject transactions for five (5) years.

### **Currency, Sale and Transportation of Negotiable Instruments**

The Company does not accept any form of physical currency (i.e., the coin or paper of the United States or any other government) from the public or its users, nor does it participate in the sale, transportation, or handling of negotiable instruments. Should XRP II decide at any time in the future to accept, sell, or transport financial instruments, the Company will establish controls to comply with all relevant record-retention and reporting requirements.

## **XRP II BSA/AML/OFAC PROGRAM**

Revised December 2015

### **POLICY VARIANCES**

Any deviation from the requirements of this Policy must be first approved by the BSA Officer. Approval may be granted in limited circumstances and cannot be granted indefinitely. The requestor must submit a written request to the BSA Officer outlining the reason(s) for the variance, the time frame for the requested variance, and the replacement controls identified to mitigate the associated risk. The BSA Officer, or designee, is responsible for tracking, maintaining and managing, all approved Policy variances.

### **POLICY ADMINISTRATION**

The BSA Officer reviews and updates the BSA/AML/OFAC Policy and Program no less than annually (more frequently when changes to the law/BSA/AML/OFAC Program/XRP II warrant). The BSA Officer consults with regulatory and legal advisors as necessary in conducting this annual review. The Compliance Oversight Committee reviews and approves the BSA/AML/OFAC Policy and Program no less than annually, or more frequently, as needed.

This BSA/AML/OFAC Policy was reviewed and approved by the Compliance Oversight Committee and became effective on December 1, 2015.

Questions or suggestions about this Policy should be forwarded to the BSA Officer, Antoinette O'Gorman at [REDACTED]@ripple.com.

---

Ripple Labs, Inc. Vendor Management Policy

---

## **Ripple Labs, Inc.**

# **VENDOR RISK MANAGEMENT POLICY**

**Owner:** Chief Compliance Officer | Antoinette O’Gorman

**Last Revised Date:** April 2016

**Contact:** Antoinette O’Gorman | [REDACTED]@ripple.com



*Ripple Labs Inc. All Rights Reserved.*

## Table of Contents

1. INTRODUCTION .....	3
3. SCOPE .....	3
4. DEFINITIONS .....	3
5. GOVERNANCE, ROLES AND RESPONSIBILITIES .....	4
6. POLICY .....	6
6.1 Vendor Risk Assessment .....	7
6.1.1 Risk Re-assessment .....	8
6.1.2 Vendor Lists .....	8
6.2 Vendor Due Diligence .....	8
7. CONTRACT MANAGEMENT .....	9
7.1 Contract Standards Checklist .....	9
7.2 Contract Negotiation .....	10
7.3 Contract Approval and Renewal .....	11
7.4 Contract Cancellation or Termination .....	11
8. ONGOING MONITORING AND VENDOR SUPERVISION .....	11
9. TRAINING .....	12
10. RECORD RETENTION .....	12
11. POLICY ENFORCEMENT EXCEPTIONS .....	12
12. POLICY ADMINISTRATION .....	13
Appendix A: Reference Materials .....	14
Appendix B: Implementation Guidelines - Reference Materials .....	15
Completing a Vendor Risk Assessment .....	15
Completing a Due Diligence Analysis .....	1
Managing the Contract .....	2
Negotiating Contracts .....	2
Evaluating Contract Language .....	3
Approving Contracts .....	4
Contract Termination .....	4
Retaining Contract Files .....	5
Supervising Vendors - Ongoing Risk Monitoring .....	5
RESPONSIBILITY .....	6



*Ripple Labs Inc. All Rights Reserved.*

## 1. INTRODUCTION

Ripple Labs, Inc., doing business as “Ripple” (or, “the Company”) is committed to applying strong oversight of its vendor service providers. Ripple requires vendors to comply with all applicable laws and regulations, as well as Ripple’s own policies. This Vendor Risk Management Policy (the “Policy”) provides guidance on how Ripple oversees and manages the risk associated with vendor activities conducted on its behalf.

Consistent with these objectives and pursuant to this Policy, Ripple has established a Vendor Risk Management Program (the “Program”) as an integral component of its compliance and risk management efforts. This Policy describes the scope of that Program and sets forth its requirements.

## 2. PURPOSE

The purpose of this Policy is to provide a framework for managing the lifecycle of vendor relationships and provide context for Ripple procedures that outline specific systems and guidelines for vendor management.

## 3. SCOPE

This Policy focuses on the risk management processes for identifying, assessing, and controlling risks associated with third-parties and applies to all Ripple business entities including individuals, departments, or subsidiaries who engage vendors as defined in this document and focuses on the risk management processes for identifying, assessing, and controlling risks associated with Ripple’s vendors.

Certain interactions with vendors and third parties are not an extension of Ripple’s business activities and do not pose meaningful risk to the Company’s safety, soundness, or compliance (for example, relationships with suppliers of office furniture or stationery or catering services). As such, these interactions are outside the scope of this Policy.

## 4. DEFINITIONS

The following definitions are provided for the purposes of this policy:

### **Vendor**

A company or individual that:

- Provides Ripple, directly or indirectly, with products or services;
- Performs functions of Ripple’s operations;



*Ripple Labs Inc. All Rights Reserved.*

- Provides shared resources like cloud computing to Ripple.

### **Contract or Agreement**

A legal document, between Ripple and a vendor, in which the vendor agrees to provide services or products and, for which, Ripple agrees to render payment.

### **Vendor Risk Rating**

A Low or High rating is assigned by Department Leaders or designated Vendor Risk Managers ('VRMs') and reviewed by Compliance as a result of the "Vendor Risk Assessment" that indicates the relative risk this vendor represents to Ripple.

High Risk service providers are providers of significant functions (e.g., hosting Ripple services or clients in third party data centers) or significant shared services (e.g., information technology), or other activities that may:

- Cause Ripple to face significant strategic, reputational, operational, legal, compliance or credit risk if the vendor fails to meet expectations;
- Cause significant customer harm;
- Require significant investment in resources to implement the vendor relationship and manage the risk; or
- Have a major impact on operations if Ripple has to find an alternate vendor or if the outsourced activity has to be brought in-house on short notice.

## **5. GOVERNANCE, ROLES AND RESPONSIBILITIES**

The following table describes the roles and responsibilities applicable to the implementation, oversight, and review of this Policy:

<b>Responsible Party</b>	<b>Role/Responsibility</b>
<b>Compliance Oversight Committee</b>	<ul style="list-style-type: none"> <li>• Review and approve this Policy at least annually;</li> <li>• Assess the effectiveness of Ripple's Vendor Risk Management Program, at least annually;</li> <li>• Review escalated issues related to this Policy.</li> </ul>
<b>Chief Compliance Officer ('CCO')</b>	<ul style="list-style-type: none"> <li>• Develop a Vendor Risk Management Program that addresses risk assessment (including the methodology), due diligence, contracting, monitoring and performance assessment, training, and documentation;</li> <li>• Implement and maintain this Policy and its related compliance testing procedures, including annual review and revision, where appropriate;</li> </ul>



*Ripple Labs Inc. All Rights Reserved.*

<b>Chief Compliance Officer ('CCO') Continued</b>	<ul style="list-style-type: none"> <li>• Communicate and interpret this Policy within Ripple as necessary to support implementation;</li> <li>• Designate Compliance staff to review vendor risk assessments;</li> <li>• Designate Compliance staff to monitor implementation of and compliance with this Policy, and recommend improvements as necessary;</li> <li>• Coordinate annual assessments of applicable vendor relationships, and review results of ongoing monitoring and annual reviews;</li> <li>• Ensure that relevant Ripple staff receive training on this Policy and that Ripple documents training and attendance;</li> <li>• Establish standards for documentation of the Company's decision-making and oversight processes for vendors;</li> <li>• Approve exceptions to this Policy, maintain a written record of exceptions including reasons for granting them, and report all such exceptions to General Counsel and the Compliance Oversight Committee; and</li> <li>• Identify and assess emerging compliance issues related to this Policy.</li> </ul>
<b>Compliance Department</b>	<ul style="list-style-type: none"> <li>• Review risk assessments and due diligence conducted for new vendor relationships and propose revisions to the CCO, if needed.</li> <li>• Review contracts to ensure that agreements or contracts meet regulatory requirements</li> </ul>
<b>Department Leaders and/or designated Vendor Risk Managers ('VRMs')</b>	<ul style="list-style-type: none"> <li>• Implement this Policy and other applicable policies and procedures within their areas of responsibility;</li> <li>• Notify Compliance and Legal of proposals for new and/or modified vendor relationships;</li> <li>• In consultation with Compliance and Legal, conduct an initial evaluation of the benefits and risks of proposed vendor relationships to determine the vendor's ability to meet the Company's objectives, requirements, and expectations,</li> <li>• Evaluate risks associated with new vendor relationships and present a risk management plan to the CCO, when applicable;</li> <li>• Conduct due diligence on proposed vendor partners;</li> <li>• Conduct ongoing monitoring and re-assessments of all vendor relationships within the department's sphere of responsibility and report any significant performance issues promptly to the CCO;</li> <li>• Ensure that Ripple and vendor staff receive compliance training appropriate to their roles and responsibilities under this Policy; and</li> </ul>



Ripple Labs Inc. All Rights Reserved.

	<ul style="list-style-type: none"> <li>Grant the CCO, or designee, unrestricted access to any business records, systems or locations necessary to fulfill the duties described in this Policy and other applicable compliance policies and procedures.</li> </ul>
<b>Legal</b>	<ul style="list-style-type: none"> <li>Interpret and advise on relevant laws and regulations;</li> <li>Review all vendor contracts and if necessary draft all proposed revisions to vendor contracts, approve and document any exceptions, and approve, along with responsible stakeholders, all contracts prior to execution; and</li> <li>Resolve escalated issues and policy exceptions related to this Policy, assisting the CCO in referring such matters to the Board and/or Compliance Oversight Committee, as necessary.</li> </ul>
<b>Chief Operations Officer ('COO')</b>	<ul style="list-style-type: none"> <li>Promote and implement a strong and proactive culture of compliance;</li> <li>Review and, where necessary, act on reports related to this Policy; and</li> <li>Hold executive management and stakeholders accountable for resolution of corrective actions related to this Policy.</li> </ul>
<b>Ripple Employees</b>	<ul style="list-style-type: none"> <li>Understand their responsibilities under this Policy;</li> <li>Identify compliance weaknesses related to this Policy within their areas of responsibility and promptly alert their department leader and Compliance; and</li> <li>Grant Compliance unrestricted access to business records, systems, or locations necessary to fulfill the duties described in this Policy and other applicable compliance policies and procedures.</li> </ul>

## 6. POLICY

It is Ripple's policy to effectively manage the lifecycle of all vendors, and ensure full compliance with requirements of applicable law and regulation regarding risk management, and vendor and contract management.

Vendor risk management, as addressed by this Policy, consists of:

- Vendor Risk Assessment
- Vendor Due Diligence
- Contract Management
- Ongoing Monitoring and Supervision



*Ripple Labs Inc. All Rights Reserved.*

The Implementation Guidelines reflected in *Appendix B* of this Policy provide best-practice guidance for effective implementation of this Policy.

## 6.1 Vendor Risk Assessment

The depth of a risk assessment varies depending on the scope, importance, and risks related to the activities under consideration for outsourcing. Evaluation of should typically address the following:

- Nature and scope of risks related to outsourcing activities;
- Impact of the proposed outsourcing on Ripple's customers;
- Importance and criticality of the activity to Ripple;
- Operational, consumer protection, and reputational risks to Ripple arising from outsourcing the proposed activity(ies);
- Ripple's ability to monitor risks related to the proposed outsourcing; and
- Strategies for effective oversight and mitigation of risks related to the proposed outsourcing. The relevant Ripple department leader, or designee, should also draft an initial plan for managing risks related to the proposed outsourcing, where applicable.

An initial risk analysis should be conducted for each potential vendor and should utilize the Vendor Risk Rating Matrix guidelines outlined below to assign a risk rating of Low or High Risk. Each vendor is assigned a risk rating by the assigned VRM based on the highest risk level attributable to the contract, or sum of all contracts, with that vendor. Exceptions to assigned risk ratings may be granted, as designated in the Risk Rating Matrix. Risk assessments are submitted to the Compliance Department for review and possible revision either prior to or accompanied by a due diligence review described below.

The assigned risk rating reflects the level of due diligence required for each vendor:

- Low Risk vendors typically require little or no further analysis or due diligence unless the vendor's services change or Ripple's use of these services changes so that the services could potentially impose more than minimal risk on Ripple's business operations as described above.

Vendor relationships meeting any of the following criteria are deemed High Risk, may require onsite due diligence reviews, and must be re-assessed on an annual basis:

- Services presenting high, consumer protection, or reputational risk as determined by the CCO;



*Ripple Labs Inc. All Rights Reserved.*

- Arrangements requiring collecting, processing, or storing large amounts of customer non-public personal information, as determined by the CCO; or
- Arrangements that are considered critical or otherwise high risk to the Company's operations, as determined by the CCO.

The following table outlines additional factors to consider when risk rating third-party vendors:

Criteria	Low	High	Exceptions Granted by
Business Impact	Nominal business impact	Mission Critical	CCO
Contract cumulative fees or annual recurring cost	<\$350,000	>\$350,000+	CCO in consultation with the COO and Chief Finance Officer ('CFO')
Contract Term	1 year or less	> 3 years	COO
Access to Non- Public Personal Information (NPPI)	No access	Access expected	VP Engineering

#### 6.1.1 Risk Re-assessment

Risk assessments should be revisited as part of contract renewal cycle or when the relationship with the vendor changes in any significant way; however, risks must be reassessed at least annually for all High Risk vendors.

#### 6.1.2 Vendor Lists

Each department will maintain a complete and up-to-date vendor list, including all Low Risk vendors. Lists must reflect the assigned risk rating for each vendor and shall be made available to the CCO for inclusion in annual Compliance reporting (of High Risk vendors) to the Compliance Oversight Committee.

### 6.2 Vendor Due Diligence

Due diligence demands reasonable inquiry into a vendor's ability to meet the requirements for the proposed service. The extent of due diligence depends on the nature, complexity, and criticality of the proposed relationship activities and the results of the initial Vendor Risk Assessment. Low Risk vendors typically require little or no ongoing due diligence unless the vendor's services change or Ripple's use of these services changes so that the services could



Ripple Labs Inc. All Rights Reserved.

potentially impose more than minimal risk on Ripple's business operations. For High Risk vendors, the review should include an evaluation of the benefits and risks of the proposed relationship to determine their ability to meet Ripple's business objectives, operational requirements, and risk management expectations. This evaluation should result in a recommendation to proceed, proceed with conditions, or to not proceed.

The Implementation Guidelines referenced in *Appendix B* to this Policy contain information that may be useful when completing the initial due diligence analysis. Records of all due diligence performed prior to establishing the vendor relationship, including determination of the vendor risk rating, must be maintained by the Vendor Relationship Manager ('VRM').

## 7. CONTRACT MANAGEMENT

A clearly drafted and legally enforceable contract provides necessary protection and structure for expectations and issue resolution.

The level of detail and relative importance of contract provisions varies with the scope and risks of services and products provided. Agreeing on necessary terms and conditions is imperative when first establishing the relationship.

### 7.1 Contract Standards Checklist

Per Federal Financial Institutions Examination Council (FFIEC) guidelines, contracts and service agreements subject to this Policy should specify and address, as applicable:

- Service or product definitions and service level expectations (performance and reliability standards);
- Technology specifications and operational responsibility;
- Confidential Information privacy and security;
- Vendor reporting and documentation standards;
- Audit rights;
- Business continuity and disaster recovery reporting and standards
- Subcontract and third party responsibility and liability;
- Detailed fee structure and billing terms; and
- General terms: liability limitations, recourse, warranties, arbitration, termination, contract expiration, assignment and indemnification.

Legal reviews all contracts prior to execution. Unless Legal, in consultation with the business function bringing the vendor into Ripple, agrees to and documents an exception, all contracts shall address the following:



*Ripple Labs Inc. All Rights Reserved.*

- The nature and scope of the arrangement between Ripple and the third-party;
- Timeframe covered by the contract;
- Performance measures and benchmarks;
- Vendor's responsibility for compliance with applicable laws, regulations, and Ripple policies and procedures regarding access to information and operations needed to ensure such compliance;
- Vendor's responsibility for providing periodic information regarding the vendor's performance under the contract and compliance with applicable laws, regulations, and Ripple policies & procedures;
- Vendor's responsibility for resolving complaints regarding the vendor's actions on Ripple's behalf;
- Circumstances that require immediate notification to Ripple, such as changes in the vendor's ownership or operational structure, adverse regulatory findings, or the filing of a lawsuit alleging material consumer protection risks;
- Compensation;
- The third-party's ability to use Ripple's information, technology, and intellectual property;
- Permissibility or prohibition of the vendor to subcontract or use another party to meet its obligations with respect to the contract, and any notice/approval requirements;
- Confidentiality and data security;
- Business continuity plans;
- Indemnification, insurance, and limits on liability;
- Dispute resolution, choice of law, default, and termination;
- Term and Termination (there should always be provisions in such contracts that allow Ripple to terminate them for cause and also for convenience to protect Ripple in case the relationship is not working out); and
- Document retention requirements.

## 7.2 Contract Negotiation

Department Leaders can delegate vendor negotiations to qualified staff with proven skills appropriate to the level of risk represented by the vendor relationship. Key areas for focused review include "audit rights" and "security requirements" clauses.

High Risk contracts, or those that are more complex or unusual in nature, must be reviewed by the following parties:

- Legal Counsel



*Ripple Labs Inc. All Rights Reserved.*

- VP of Engineering - review required for all contract negotiations related to software, hardware, and Information Systems
- Compliance Manager – review to ensure that agreement or contract meets regulatory requirements
- Director of Risk Management – review to ensure that agreement or contract does not expose Ripple to unnecessary risk.

### **7.3 Contract Approval and Renewal**

Contracts between Ripple and its vendors are the basis for effective management of relationships by specifying expectations and performance standards applicable to both parties and defining the oversight framework.

Ripple ensures that it executes written contracts with all of its vendors. Although contracts vary with the scope and risks of the relationship, all contracts take into account the business requirements and key risk factors identified during the vendor risk assessment and due diligence processes. Ripple's Legal Department is responsible for ensuring that contracts are fair, and do not expose Ripple to undue risk, or favor the vendor to the extent that they are one sided. The goal of the Legal Department is to make certain that Ripple's interests are represented in these contracts by, among other things, seeking to make the rights and obligations of the parties mutual. The business function contracting with the vendor will ensure that the contract includes sufficient detail to provide Ripple assurances for performance, reliability, and reporting commensurate with the risks to the Company.

Department Leaders are responsible for contracts executed by their staff. All High Risk vendor contracts, including renewals, must be executed by VP level or higher. Department Leaders or their designated VRMs are responsible for ensuring that all High Risk contracts are reviewed at least annually and, if necessary, with assistance from Legal, are updated to reflect any changes in Ripple's operations, regulatory requirements, and other factors.

### **7.4 Contract Cancellation or Termination**

Cancellation or termination of contracts must follow agreed upon contract language and be executed at the same or higher level of the organization as the original contract execution. Always confer with Legal prior to cancellation or termination of any contracts.

## **8. ONGOING MONITORING AND VENDOR SUPERVISION**

Each vendor is assigned a designated VRM responsible for completing the vendor risk analysis, the vendor due diligence review and subsequent annual reviews, maintaining vendor files, and acting as vendor liaison.



*Ripple Labs Inc. All Rights Reserved.*

The VRM's ongoing risk monitoring is required to keep abreast of any significant changes to the vendor environment. Areas to monitor include, but are not limited to, the company's financial health, business continuity plans, and security controls. A substantial or sudden change in any of these areas could significantly increase the risk the vendor poses to the organization.

In addition to the factors identified in the initial risk assessment, annual reviews of all High Risk vendors should include:

- A review the vendor's performance in the past year relative to service level agreements to determine whether the vendor has met its contractual terms and conditions;
- A determination whether any revisions to the service level agreements are needed based on Ripple's changing business needs, new regulatory requirements or expectations, and technological developments;
- Evaluation of the vendors financial condition and assessment of its capacity to continue performing under the terms of the contract and service level agreement(s);
- Consideration of a change in its risk status, where warranted;
- Whether the relationship continues or is terminated; and
- Review of any other key contractual provisions.

The Chief Compliance Officer will provide an annual status report of High Risk vendors to the Compliance Oversight Committee.

## 9. TRAINING

As part of Ripple's training program, the CCO or designee annually assesses training requirements for Ripple staff involved in risk assessment, due diligence, contracting, monitoring and overseeing vendor relationships. Based on the assessment, the CCO oversees the development of training materials, training completion, and retention of training records.

## 10. RECORD RETENTION

All records of vendor contract files will be retained in accordance with applicable state and federal regulations, as well as Ripple's own policies, and will be maintained by Ripple for a minimum of five (5) years after termination of the contract.

## 11. POLICY ENFORCEMENT EXCEPTIONS

The CCO reviews and authorizes exceptions to this Policy. Exceptions are reported to the



*Ripple Labs Inc. All Rights Reserved.*

Compliance Oversight Committee on an as needed basis.

## 12. POLICY ADMINISTRATION

At least annually, the CCO reviews this Policy and related procedures and recommend appropriate changes. The review includes consideration of feedback on the effectiveness of the Policy.

Any changes to this Policy must be approved by the Compliance Oversight Committee, which reviews and approves this Policy at least annually.

Any conflicts between this Policy and Ripple's other legal obligations should be submitted immediately to the CCO for further evaluation and/or subsequent submission to Legal.

Questions or suggestions concerning this Policy should be forwarded to the CCO.



*Ripple Labs Inc. All Rights Reserved.*

## Appendix A: Reference Materials

### **FDIC Guidance for Managing Third-Party Risk (FIL 44-2008)**

This guidance provides a general framework that senior management may use to provide appropriate oversight and risk management of significant third-party relationships.

### **FFIEC Outsourcing Technology Booklet**

The booklet provides guidance on evaluating risk management processes to establish, manage, and monitor IT outsourcing relationships.

### **FFIEC Outsourced Cloud Computing Guidance**

The guidance considers cloud computing to be a form of outsourcing subject to the risk management requirements applicable to third-party relationships.



*Ripple Labs Inc. All Rights Reserved.*

## Appendix B: Implementation Guidelines - Reference Materials

Appendix B provides guidelines for effective implementation of the Vendor Management Policy and is employed as directed by the appropriate department Vice President, or designated VRM.

### Completing a Vendor Risk Assessment

1. Assign a Vendor Risk Rating using the Vendor Risk Rating Matrix in section 6.1 of the Vendor Management Policy.
2. Review any substantive risk exposure to Ripple if the product or service fails or performs inadequately:

Risk Exposure Category Considerations	
Regulatory	<ul style="list-style-type: none"> <li>• Can the vendor create regulatory risk for Ripple?</li> </ul>
Reputation	<ul style="list-style-type: none"> <li>• Can the vendor impact Ripple's reputation?</li> </ul>
Financial	<ul style="list-style-type: none"> <li>• Can the vendor impact Ripple or its members financially?</li> <li>• Does Ripple or the vendor have insurance that will allow Ripple to transfer some of the risk?</li> </ul>
Sensitive Data Access	<ul style="list-style-type: none"> <li>• To what extent will the vendor handle sensitive Ripple data?</li> </ul>
Operational Effectiveness Process Risk People Risk System Risk	<ul style="list-style-type: none"> <li>• How would the vendor's failure impact Ripple's business needs and strategic objectives?</li> <li>• Could Ripple step in and perform the critical functions provided by the vendor if the vendor failed to perform?</li> <li>• Are there other potential vendors that could readily assume service should the current provider fail?</li> <li>• Can Ripple provide adequate oversight of the vendor's function?</li> <li>• Can the vendor create risk to Ripple's processes, people, or systems?</li> <li>• Would Ripple be considered the "Controlling Employer" for this vendor?</li> <li>• Would Ripple be placed in a position of "Joint Employer's Liability" for this vendor?</li> </ul> <p>Note: The terms "Controlling Employer" and "Joint Employer's Liability" usually apply to staff employed by an outside company, such as a staffing agency, but whose work place activities are directed by Ripple. Direct questions regarding these designations to the Director of Risk Management.</p>



Ripple Labs Inc. All Rights Reserved.

## Completing a Due Diligence Analysis

Ripple must take appropriate steps to ensure that third-party vendors do not pose unwarranted risks to consumers. These steps should include, at a minimum:

- Conducting due diligence (including an objective assessment, commensurate with the risk and complexity of the activities) prior to selecting the vendor specifically to verify that the third party vendor understands and is capable of complying with applicable laws and regulations.
- For all High Risk vendors, requesting and reviewing policies, procedures, internal controls, and training materials to ensure proper training and oversight over employees or agents who have consumer contact or compliance responsibilities
- Including in the vendor contract clear expectations of compliance and enforceable consequences for violating compliance or compliance-related responsibilities such as unfair, deceptive, or abusive acts or practices
- Establishing internal controls including procedures for ongoing monitoring and reporting, risk management disaster recovery strategies, where applicable
- Taking prompt action to address problems when identified, including terminating relationships where appropriate.

In addition to coordinating the above, due diligence evaluation conducted by the VRM, in collaboration with appropriate parties, may also include review of the proposed vendor's:

- Business strategy and goals;
- Financial condition;
- Legal and regulatory compliance;
- Business experience and reputation;
- Fee structure and incentives;
- Qualifications, backgrounds, and reputations of principals;
- Risk management program and performance;
- Information security program and performance;
- Business processes and systems;



*Ripple Labs Inc. All Rights Reserved.*

- Reliance on subcontractors;
- Contractual relationships that may affect the vendor's ability to perform activities on Ripple's behalf or shift liability to Ripple;
- Physical security and resilience with respect to business disruptions or disasters;
- Human resource management, including qualifications of those who perform activities on Ripple's behalf; and
- Insurance coverage.

Any risks identified must be reviewed internally. The vendor should be requested to correct identified areas of weak control. Corrections should be tested to ensure compliance with Company requirements and periodically re-examined.

All analysis and due diligence must be recorded and retained centrally within the Vendor Relationship Manager records.

## Managing the Contract

Vendor relationship documentation varies with the scope and risks of the services and products provided. The process includes:

- Negotiating the Contract
- Reviewing the Contract Language
- Approving and Renewing the Contract
- Contract Cancellation or Termination
- Retaining Contract Files

## Negotiating Contracts

This process is completed by designated qualified staff with proven skills appropriate to the level of risk represented by the vendor relationship.

1. Review each contract from four perspectives:

Perspective	Consideration
Legal	<ul style="list-style-type: none"> <li>• Are Ripple's interests adequately protected if a problem arises with this vendor?</li> </ul>



*Ripple Labs Inc. All Rights Reserved.*

Financial	<ul style="list-style-type: none"> <li>Does the agreement reasonably assure that Ripple's investment in this relationship will deliver the desired benefits without exposing Ripple to unacceptable financial risks?</li> </ul>
Operational	<ul style="list-style-type: none"> <li>Are the terms, examples of which are referenced below, of the agreement operationally feasible for Ripple? <ul style="list-style-type: none"> <li>– Timing considerations</li> <li>– Service levels commitments</li> <li>– Ripple performance commitments</li> <li>– Technology compatibility</li> </ul> </li> </ul>
Compliance and Risk	<ul style="list-style-type: none"> <li>Are the terms of the agreement acceptable in light of regulatory, financial, operational, and reputation</li> </ul>

- Complete the levels of review as directed in 7.2 of this Policy.
- Maintain multiple vendor candidates where possible for leverage at the contract negotiation stage.
- Record negotiations and contact between a potential vendor and the Ripple using *Track Changes* function, or similar tool.
- Retain negotiation records in the centralized vendor management database for the life of the contract.

## Evaluating Contract Language

- Verify that contractual or agreement language meets regulatory requirements and does not expose Ripple to unnecessary risk.
- Verify that essential components of the agreement include:
  - Performance standards, expectations, and responsibilities
  - Fees and payment terms
  - Term length
  - Termination provisions
  - Insurance Requirements
- Evaluate the agreement also for what it *does not state*, in addition to written content.
- Verify that the vendor's standard agreement includes all necessary clauses.
- Consider the appropriateness of the following contractual clauses:
  - Definitions
  - Scope of work



Ripple Labs Inc. All Rights Reserved.

- Process for changing scope of work
- Installation and training requirements
- Ownership of any work product or intellectual property
- Acknowledgement that the vendor is subject to regulatory review
- Privacy and information security
- Confidentiality Agreement
- Limitations of liability
- Indemnity
- Warranties
- Standard Ripple dispute resolution provisions
- Choice of law
- Choice of venue
- Service Level Agreement including
  - Acceptable range of service quality and applicable timeframes
  - Definition of what is being measured
  - Formula for calculating the measurement
  - Mechanism for ongoing monitoring, and supervision
  - Type and timing of reporting on the status of performance
  - Penalties or credits for meeting, exceeding, or failing to meet targets

## **Approving Contracts**

Execute the contract with the appropriate level of approval as outlined in section 7.3 of the Vendor Management Policy.

When a contract is due for renewal, complete the following:

- a) Review and update the Vendor Risk Rating
- b) Review and update the Vendor Due Diligence Report
- c) Review contract terms

## **Contract Termination**

When cancelling a contract, follow agreed upon contract language and execute at



*Ripple Labs Inc. All Rights Reserved.*

the same or higher level of the organization as the original contract execution.

### Retaining Contract Files

Complete the following based upon file type:

File Type	Action
Department Vendor	Maintain complete list of risk-rated vendors
Original Vendor Contract File	Retain originals of all contracts, agreements, and other essential vendor relationship documentation in the centralized file location for four years after contract expiration.
Working Vendor	Retain copies of all negotiation records, contracts, agreements, and related documentation in the VRM's work

### Supervising Vendors – Ongoing Risk Monitoring

The VRM completes the following steps:

1. Assigns Vendor Risk Rating using the Vendor Risk Rating Matrix
2. Completes Vendor Due Diligence Analysis, as appropriate for the risk rating
3. Completes periodic due diligence review (at least annually for High Risk vendors)
4. Coordinates and documents ongoing vendor communication
5. Maintains vendor files
6. Compiles and maintains vendor information, including:
  - Vendor name and contact information
  - Service or product provided
  - Risk rating
  - Contract expiration
  - Renewal dates and terms
  - Regulatory requirements
  - Insurance Requirements
  - Required vendor reports
  - Date of last review and next review



*Ripple Labs Inc. All Rights Reserved.*

- Triggers for annual and interim reviews
  - Contract amount
  - Number of licenses, if applicable
7. Monitors vendor compliance to contract terms
  8. Coordinates contract renewal with appropriate contract approver
  9. Coordinates contract cancellation

## **RESPONSIBILITY**

Each department Vice President is responsible for implementing these guidelines as appropriate to the department.

The designated VRM is responsible for adhering to the implementation guidelines as directed by the department Vice President.



*Ripple Labs Inc. All Rights Reserved.*